BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平９－３０７５４２

(43)公開日　平成９年（１９９７）１１月２８日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 9/08			H04L 9/00	601 B	
G09C 1/00	630	7259-5J	G09C 1/00	630 B	
		7259-5J		630 E	
			H04L 9/00	601 E	

審査請求　未請求　請求項の数８　ＯＬ　（全１６頁）

(21)出願番号　特願平８－１５４６８８

(22)出願日　平成８年（１９９６）６月１４日

(31)優先権主張番号　特願平８－５９７４６

(32)優先日　平８（１９９６）３月１５日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　０００００２１８５
ソニー株式会社
東京都品川区北品川６丁目７番３５号

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

(72)発明者　石井　眞
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

(72)発明者　窪田　一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

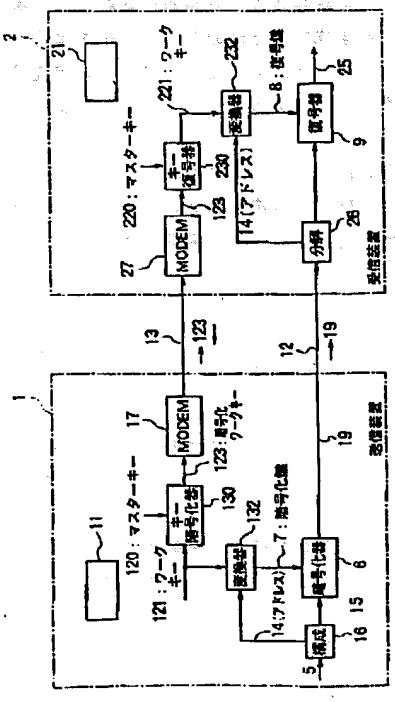
(74)代理人　弁理士　佐藤　隆久

(54)【発明の名称】データ伝送装置とその方法

(57)【要約】

【課題】　暗号鍵または復号鍵の伝送の安全性を高めて、暗号化伝送データの漏洩に対する安全性を高めるデータ伝送装置を提供する。

【解決手段】　大容量のデータを伝送する衛星回線伝送路などの大容量伝送路１２と、暗号鍵または復号鍵あるいはこれらの生成のための情報を伝送する公衆電話回線などの小容量伝送路１３を設ける。暗号化セッション鍵をワークキーと送信先の受信装置２の宛先アドレスとを用いて変換する。また復号用セッション鍵を自己のアドレスとワークキーを用いて変換する。ワークキーは好ましくは、暗号化されて小容量伝送路１３を伝送される。送信装置１において、伝送すべきデータ５を上記のごとく変換した暗号セッション７を用いて暗号化する他、宛先データなどの伝送制御情報を付加して大容量伝送路１２を経由して受信装置２に伝送する。受信装置２において、上記のごとく変換した復号セッション鍵８を用いて暗号化データ１９を復号する。



1

【特許請求の範囲】

【請求項1】大量のデータを高速で伝送可能な第1の伝送系統と、

有線形式の第2の伝送系統と、

前記第1の伝送系統と前記第2の伝送系統を介して接続されている第1の伝送装置と第2の伝送装置とを有し、

前記第1の伝送装置が前記第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第2の伝送装置に伝送し、

前記第1の伝送装置が、暗号化データを送信する前記第2の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第1の伝送系統に送出し、

前記第2の伝送装置は前記第1の伝送系統から受信したデータから前記宛先データを取り出し、該宛先データと前記第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送装置。

【請求項2】前記宛先アドレスは複数の装置のグループを示すアドレスである、請求項1記載のデータ伝送装置。

【請求項3】前記第1の伝送系統は衛星回線伝送路である、請求項1または2記載のデータ伝送装置。

【請求項4】前記第1の伝送装置は、前記第2の伝送系統を介して前記第2の伝送装置に伝送する、復号化セッション鍵を生成するためのワークキーを暗号化して伝送し、

前記第2の伝送装置は、該暗号化されている復号化セッション鍵を生成するためのワークキーを復号し、該復号したワークキーと前記宛先データを用いて復号化セッション鍵を生成する請求項1～3いずれか記載のデータ伝送装置。

【請求項5】大量のデータを高速で伝送可能な第1の伝送系統および有線形式の第2の伝送系統に接続され、

ワークキーを前記第2の伝送系統に送出する第1の送出手段と、

ワークキーと送信先のアドレスとから暗号化セッション鍵を生成する鍵変換手段と、

前記生成した暗号化セッション鍵を用いて伝送すべきデータを暗号化するデータ暗号化手段と、

該暗号化伝送データに、送信先のアドレスを付加して前記第1の伝送系統に送出する送出手段とを有するデータ伝送装置。

【請求項6】大量のデータを高速で伝送可能な第1の伝送系統と、有線形式の第2の伝送系統とを用いて第1の伝送装置と第2の伝送装置との間で暗号化データを伝送するデータ伝送方法であって、

2

前記第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第2の伝送装置に伝送し、

暗号化データを送信する前記第2の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッションキー鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第1の伝送系統に送出し、

前記第1の伝送系統から受信したデータから前記宛先データを取り出し、該宛先データと前記第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送方法。

【請求項7】前記宛先アドレスは複数の装置のグループに対するアドレスである、請求項6記載のデータ伝送方法。

【請求項8】大量のデータを高速で伝送可能な第1の伝送系統と、

有線形式の第2の伝送系統と、

前記第1の伝送系統と前記第2の伝送系統を介して接続されている第1の伝送装置と第2の伝送装置とを有し、

前記第1の伝送装置が前記第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第2の伝送装置に伝送し、

前記第1の伝送装置が、前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第1の伝送系統に送出し、

前記第2の伝送装置は前記第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデータを伝送するデータ伝送装置とその方法に関するものであり、特に、大量のデータを暗号化して送受信する場合に用いる暗号鍵および復号鍵の管理を適切に行うデータ伝送装置とその方法に関する。

【0002】

【従来の技術】公衆電話回線、専用回線などを用いてデータ伝送する場合または通話する場合、伝送情報の漏洩を防止するためまたは伝送情報に対する攻撃（妨害）に対して情報の信頼性を維持するため、平文のデータを暗号化し（スクランブルし）て伝送し、受信先で暗号化されたデータを復号して（デスクランブルして）いる。代表的な暗号方式としては共通鍵暗号方式と公開鍵方式と

が知られている。共通鍵暗号方式は対称暗号系とも呼ばれており、アルゴリズム非公開型とアルゴリズム公開型とが知られている。アルゴリズム公開型の代表的なものとしてＤＥＳ（Data Encryption Standard）が知られている。公開鍵方式は、検査鍵から生成鍵を導出するために莫大な計算量が必要なため実質的に生成鍵が解読されないので、暗号鍵を公開してもよい暗号方式であり、非対称鍵暗号方式とも呼ばれている。

【０００３】暗号化方式は伝送データが伝送される回線系統の種別、伝送データの機密度（秘密性）、伝送データの量などに応じて決定される。専用回線を用いたデータ伝送においては、情報の漏洩、伝送データへの攻撃の度合いは低いが、公衆電話回線を用いてデータ伝送する場合は情報の漏洩の度合い、攻撃の度合いは高くなる。さらに衛星放送回線を用いたデータ伝送は、不特定多数の装置で受信可能であるから情報の漏洩の度合いは一層高くなる。

【０００４】図１は伝送路上のデータを共通鍵暗号化方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。図１の暗号化データ伝送装置において、符号１は送信装置（送信者）を示し、２は受信装置（受信者）を示し、３は盗聴装置（盗聴者）を示し、４はデータ伝送路を示し、５は伝送すべきデータを示し、６は送信装置１内に設けられた暗号化器を示し、７は暗号化器６で暗号化に用いる暗号化鍵（暗号化用セッションキーという）を示し、８は復号鍵（復号用セッションキーという）を示し、９は復号鍵を用いてデータ伝送路４から受信した暗号化データを復号する復号器を示し、１０は復号後のデータを示す。送信装置１において、データ５を伝送路４上に送出する際に、暗号化器６において暗号化鍵７を用いてデータ５を暗号化し、暗号化したデータを伝送路４を経由して受信装置２に送出する。受信装置２において、伝送路４から暗号化されたデータを受信したら、復号器９において暗号鍵７に対応する復号鍵８を用いて受信した暗号化されたデータを復号し、目的とする復号（解読）データ１０を得る。この例においては、盗聴装置３が伝送路４から受信装置２と同様に暗号化されたデータを受信しても、復号鍵８がないのでこれを正しく復号することが困難である。すなわち、盗聴装置３ではそのままでは意味不明のスクランブルのかかったデータを扱うことになるから、現実的に盗聴装置３側に情報が漏洩することを防いでいる。この例における共通鍵暗号方式の主要な暗号化方式では、一般に暗号化鍵と復号鍵は同一のビット列である。

【０００５】最近、特定の契約者との間にのみＴＶ番組を提供する衛星放送が行われている。衛星放送に用いる伝送系統は、映像と音声という大量のデータ（情報）を短時間で伝送することが可能である。また人工衛星を用いた伝送系統は、大量の情報を短い時間で伝送することが可能であるため、放送に限らず、コンピュータ・データなどのデータの伝送に広く利用されている。しかしながら、人工衛星を用いた伝送においては、電話回線、専用回線などの１対１通信方式と異なり、不特定多数の多くの受信者が（受信装置で）容易に受信できるので、盗聴されやすいという面も有している。その結果、たとえば、有料衛星放送が盗聴される可能性が高い。そこで、ＴＶ放送の映像データ、音声データについても暗号化して伝送することが提案されている。実際の伝送においては全てのデータについて暗号化処理をする訳ではなく、送信装置において伝送すべきデータの内容に応じて、暗号化すべきデータを暗号化して伝送路上に送出し、受信者は暗号化されたデータの全部または一部を復号し、その結果得られた情報により、現在その全部または一部が復号されたデータが自分にとって必要なものであるか否かを知る。

【０００６】このように暗号化したデータを伝送する暗号化データ伝送装置において、送信側と受信側とで、事前に暗号鍵と復号鍵を秘密に持つ必要がある。送信側で暗号鍵を持ち受信側で復号鍵を持つ従来の方法としては、たとえば、衛星回線伝送路を用いて映像データなどを暗号化して伝送する場合には、送信者が受信者に復号鍵を記録した紙やＩＣカード等を郵送等の方法で送る方法と、衛星回線伝送路を暗号鍵と復号鍵を伝送する方法、さらにこれらを組み合わせた方法が考えられる。

【０００７】

【発明が解決しようとする課題】暗号鍵と復号鍵の従来の管理方法には下記に挙げる問題がある。第１の問題は、送信者による暗号化鍵の所有のしかた、あるいは受信者による復号鍵の所有のしかたに関係した問題である。上述したように、送信者が暗号化鍵を持ち受信者が復号鍵を持つための方法としては、送信者が受信者に復号鍵を記録した紙、ＩＣカードなどの物体を郵送等の方法で送る方法と、衛星回線伝送路を用いて送る方法、さらにこれらを組み合わせた方法が一般的である。

（１）復号鍵を記録した物体を郵送等で送る方法においては、その手続きの繁雑さから暗号化鍵および復号鍵の変更が容易に行えない。そのため多くのデータに対して同一の鍵を用いて暗号化したデータを伝送路上に送出することになり、盗聴者により多くの情報を与えるという意味で、暗号解読に対しての安全性が低い。

（２）復号鍵を衛星回線伝送路を用いて送る方法においては、衛星回線伝送路上のデータは、その者を送信者が受信者として希望するか否かにかかわらず、アンテナ等の機材を持つ不特定多数の者に受信されることから、送信者が希望する受信者以外の者に復号鍵を知られてしまう可能性があるので、伝送の安全が保てないという課題がある。

（３）上記２つの方法を組み合わせる方法、つまり、郵送等で送られた物体に記録してある情報と、衛星回線伝送路を伝送された情報から復号鍵を作成する方法におい

5

ては、２つの方法の欠点が補われ、この伝送方法の安全性はある程度強いものになる。しかし、たとえば、衛星回線伝送路上のデータを受信でき、かつ、郵送等で他人に送られた情報をなんらかの方法で知りえた者は、この他人が用いる復号鍵を知り、暗号化されている衛星回線伝送路上の他人宛のデータの復号ができることになり、依然として情報が漏洩するという問題がある。

【０００８】第２の問題は送信者がデータを暗号化するか否かを、あるいは、受信者が受信したデータを復号するか否かをいかにして判断するかに関する。上述したように、現在一般的に用いられている方法では、送信装置においてデータの内容を見て暗号化する必要のあるデータを暗号化して伝送路上に送信し、受信装置においては伝送路から受信した暗号化されたデータの全部または一部を復号して得られた情報により、このデータが自分にとって必要であるか否かを判断する。しかしこの方法では、送信装置において、データが暗号化する必要のあるものか否かを知るためにその内容を知るための処理と、受信装置において受信した暗号化されたデータは自分の必要とするものであるか否かを判断するために暗号化されたデータの全部または一部を復号するための処理が必要である。そのためにはより高速に伝送を行う必要があるが、これまでの装置構成ではその要望を満足できなかった。

【０００９】本発明の目的は、送信側において有効に伝送データを暗号化し、受信側において伝送された暗号化データを有効に復号できるデータ伝送装置とその方法を提供することにある。

【００１０】

【課題を解決するための手段】本発明においては、送信側が、ワークキーとを用いて暗号化セッション鍵を生成する、好適には、受信側の宛先アドレスとワークキーとを用いて暗号化セッション鍵を生成して、その鍵を用いて伝送データを暗号化して、第１の伝送系統を介して送出する。送信側から受信側に第２の伝送系統を介してワークキーを伝送しておく。受信側では、ワークキーを用いて、または好適には宛先アドレスとワークキーとを用いて復号化セッション鍵を生成し、この鍵を用いて伝送データを復号する。本発明は、第２の課題を解決するために、送信者がデータを暗号化するか否かを、あるいは、受信者が受信したデータを復号するか否かを、データを伝送するための制御情報によって判断する。本発明においては、大量のデータを高速かつ効率よく伝送可能な衛星放送伝送系統（伝送路）などの大容量伝送路（第１の伝送系統）と、この大容量伝送路とは独立に、ワークキーの授受を行う公衆電話回線などの小容量伝送路（第２の伝送系統）を用いる。小容量伝送路としては、漏洩に対する機密性を高めるため、送信装置と受信装置との間の通信が１対１で行える有線通信路が好ましい。

【００１１】したがって、本発明によれば、大量のデータを高速で伝送可能な第１の伝送系統と、有線形式の第２の伝送系統と、第１の伝送系統と第２の伝送系統を介して接続されている第１の伝送装置と第２の伝送装置とを有し、第１の伝送装置が第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを第２の伝送装置に伝送し、第１の伝送装置が、暗号化データを送信する第２の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、宛先データを付加して第１の伝送系統に送出し、第２の伝送装置は第１の伝送系統から受信したデータから宛先データを取り出し、該宛先データと第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて暗号化伝送データを復号するデータ伝送装置が提供される。宛先アドレスとしては、単一の装置を示す場合に限らず、複数の装置のグループを示すこともできる。

【００１２】好適には、第１の伝送系統は衛星回線伝送路である。また好適には、第１の伝送装置は、第２の伝送系統を介して第２の伝送装置に伝送する、復号化セッション鍵を生成するためのワークキーを暗号化して伝送し、第２の伝送装置は、該暗号化されている復号化セッション鍵を生成するためのワークキーを復号し、該復号したワークキーと前記宛先データを用いて復号化セッション鍵を生成する。

【００１３】また本発明によれば、大量のデータを高速で伝送可能な第１の伝送系統および有線形式の第２の伝送系統に接続され、ワークキーを第２の伝送系統に送出する第１の送出手段と、ワークキーと送信先のアドレスとから暗号化セッション鍵を生成する鍵変換手段と、生成した暗号化セッション鍵を用いて伝送すべきデータを暗号化するデータ暗号化手段と、該暗号化伝送データに、送信先のアドレスを付加して第１の伝送系統に送出する送出手段とを有するデータ伝送装置が提供される。

【００１４】さらに本発明によれば、大量のデータを高速で伝送可能な第１の伝送系統と、有線形式の第２の伝送系統とを用いて第１の伝送装置と第２の伝送装置との間で暗号化データを伝送するデータ伝送方法であって、第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを第２の伝送装置に伝送し、暗号化データを送信する第２の伝送装置の宛先データおよび暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッションキー鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、宛先データを付加して第１の伝送系統に送出し、第１の伝送系統から受信したデータから宛先データを取り出し、該宛先データと第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて暗号化

7

伝送データを復号する、データ伝送方法が提供される。

【００１５】

【発明の実施の形態】

【実施例１】本発明のデータ伝送装置の第１実施例について、図２を参照して述べる。図２は本発明のデータ伝送装置の第１実施例の概念的な構成図である。図２に図解した第１実施例のデータ伝送装置において、符号１は送信装置（送信者、または第１の伝送装置）を示し、２は受信装置（受信者または第２の伝送装置）を示し、３は送信装置１および受信装置２を除く第３者の受信装置を示し、１２は第１の伝送系統としての大容量伝送路を示し、１３は第２の伝送系統としての小容量伝送路を示す。

【００１６】本発明においては、大容量伝送路１２を介してＴＶ信号、コンピュータデータなどの大量のデータを伝送する。大容量伝送路１２としては、大量のデータを高速かつ効率よく伝送する衛星回線伝送路が好ましい。また、暗号または復号に関する情報を伝送する小容量伝送路１３としては、衛星回線伝送路より情報の漏洩が少ない１対１通信を行う、有線伝送路、たとえば、公衆電話回線、専用回線などが望ましい。以下の実施例においては、小容量伝送路１３として公衆電話回線を用いた場合を例示する。

【００１７】図３は大容量伝送路１２として衛星回線伝送路を用い、小容量伝送路１３として公衆電話回線を用いた伝送路の概略構成を示す図である。衛星回線伝送路１２は、送信用アンテナ１２０、空中伝送路１２１、中継器を内蔵した人工衛星１２２、空中伝送路１２３、および、受信用アンテナ１２４から構成されている。送信用アンテナ１２０には、送信装置１に設けられた送信機（ＴＸ）１０が接続され、受信用アンテナ１２４には受信装置２に設けられた受信機（ＲＸ）２０が接続されている。受信機２０としては、たとえば、ＴＶ映像信号を受信する場合は、ＴＶ受像機内の受信機である。なお、アンテナ１２０、１２４は送信用だけでなく受信用にも用いることができる。送信装置１内の送信機（ＴＸ）１０、受信装置２内の受信機（ＲＸ）２０はそれぞれ送受信機として、送信も受信も可能な装置を設けることができる。特に、大容量伝送データとして、コンピュータデータを伝送する場合などは、相互に送受信する場合が多いから、送信装置１および受信装置２にそれぞれ送受信機を設けておくことが望ましい。公衆電話回線１３は、送信装置１内に変復調器（ＭＯＤＥＭ：モデム）１７を設け、受信装置２内にも変復調器（モデム）２７を設けておき、これら変復調器１７，２７相互で、電話線１３１、交換機（ＥＸ）１３０、電話線１３２を介して暗号鍵などのデータの伝送を行う。以下、大容量伝送路１２としては、図３に図解した衛星回線伝送路１２、小容量伝送路１３として図３に示した公衆電話回線１３を例示する。

8

【００１８】送信装置１が大容量伝送路１２に送出した暗号化したデータを、大容量伝送路１２と無線接続されている受信装置２に送信する。本実施例においては、送信装置１は大容量伝送路１２を用いて、伝送すべきデータをインターネット・プロトコル（INTERNET Protocol: インターネット通信規約）ＩＰを用いて伝送する。なお通信規約としては、インターネット・プロトコルＩＰに限らず、後述するように、たとえば、ＡＴＭ（Asynchronous Transfer Mode、非同期転送モード）など、その他の通信規約を用いることもできる。ただし、以下の実施例においては、インターネット・プロトコルＩＰについて例示する。インターネット・プロトコルＩＰは、データの伝送における代表的なプロトコルであり、その詳細はたとえば、西田竹志著の文献、ＴＣＰ／ＩＰ　インターネットワーキング、株式会社、ソフト・リサーチ・センター発行、に示されている。

【００１９】図４はインターネット・プロトコルＩＰにおけるメッセージ伝送の単位であるＩＰデータグラム１５の概略図である。符号５は伝送すべきデータを示し、１４はＩＰヘッダを示し、１５はメッセージ伝送の１単位であるＩＰデータグラムを示す。インターネット・プロトコルＩＰに従えば伝送すべきデータ５に、伝送に必要な制御情報であるＩＰヘッダ１４が付加され、全体がＩＰデータグラム１５を構成する。本実施例においては、ＩＰヘッダ１４には、送信装置１からデータを伝送する宛先データ（すなわち、受信装置２の宛先データ）、および、伝送すべきデータ５を暗号化するか否かのフラグがセットされる。ＩＰヘッダ１４に規定される宛先データおよび暗号化するか否かの情報を伝送制御情報と呼ぶ。

【００２０】<u>データ伝送装置の構成</u>

図５は図２に図解した本発明の暗号化データ伝送装置の第１実施例についてインターネット・プロトコルＩＰを適用して実現したより詳細な構成を示す図である。暗号化データ伝送装置は、大容量伝送路１２（具体的には、図３に図解した大容量伝送路１２）と小容量伝送路１３（具体的には、図３に図解した公衆電話回線１３）を介して接続されている送信装置１と受信装置２とを有している。送信装置１には、図４に図解したように伝送すべきデータ５にＩＰヘッダ１４を付加してＩＰデータグラム１５を形成するＩＰデータグラム構成器１６と、暗号鍵７を用いてＩＰデータグラム１５を暗号化して暗号化データ１９を生成する暗号化器６が設けられている。衛星回線伝送路１２には、図示しない送信機１０（図３参照）を用いて暗号化器６で暗号化された暗号化データ１９とＩＰデータグラム構成器１６から出力されて暗号化されていない平文データ１８とが伝送される。送信装置１にはさらに、公衆電話回線１３を介して復号鍵の伝送を行う変復調器（モデム）１７と、送信装置１内の信号処理および制御処理を行う信号処理装置１１とが設けら

れている。信号処理装置１１は、たとえば、コンピュータを用いて構成されている。信号処理装置１１はＩＰデータグラム構成器１６、暗号化器６および変復調器（モデム）１７の全体処理および制御を行う。受信装置２には、データグラム分解器２６、復号器９、信号処理装置２１、変復調器（モデム）２７が設けられている。

【００２１】送信装置１の動作

送信装置１において、ＩＰデータグラム構成器１６が伝送すべきデータ５にＩＰヘッダ１４を付加してＩＰデータグラム１５を生成する。この際に、送信装置１の信号処理装置１１はＩＰヘッダ１４中の宛先アドレスの部分を用いて、伝送データ５を暗号化するか否かを判断し、暗号化する場合には、ハードウェアとして構成された暗号化器６を用いて暗号化鍵（暗号化用セッションキー）７を鍵として伝送すべきデータ５を暗号化し、暗号化データ１９を衛星回線伝送路１２に送出する。なお、暗号鍵７は、送信装置１内の信号処理装置１１が上記宛先アドレスに基づいて生成する。伝送データ５を暗号化しない場合には、送信装置１は暗号化されていないＩＰデータグラム（平文データ）１８を衛星回線伝送路１２に送出する。

【００２２】図６は、上記の送信装置の主要な処理の流れを示すフローチャートである。ステップＳ１において送信装置１のＩＰデータグラム構成器１６は伝送すべきデータ５にＩＰヘッダを付加してＩＰデータグラムを生成する。ステップＳ２において、送信装置１の暗号化器６はＩＰヘッダ１４に含まれる宛先アドレスを見てデータを暗号化するか否かを判断する。暗号化する場合にはステップＳ３へ進み、暗号化器６は暗号鍵７を用いて伝送すべきデータ５に対して暗号化処理を行う。その後、ステップＳ４へ進み、送信装置１の送信機１０（図示せず）は暗号化したデータを衛星回線伝送路１２に送出する。暗号化しない場合には、ステップＳ４に進み、送信装置１の送信機１０（図示せず、図３参照）は暗号化しない平文データ１８を衛星回線伝送路１２に送出する。信号処理装置１１はこれらの動作処理および制御を行う。

【００２３】復号鍵８の伝送

衛星回線伝送路１２を用いたデータの伝送とは別に、公衆電話回線１３を用いて、信号処理装置１１と変復調器（モデム）１７、および、信号処理装置２１と変復調器（モデム）２７との間で、送信装置１から受信装置２に暗号鍵７に対応する復号鍵８を伝送しておく。これにより、暗号鍵７に対応した復号鍵８を用いれば受信装置２において暗号化データ１９の復号が可能になる。

【００２４】受信装置２の動作

受信装置２において、図示しない受信機２０（図３参照）で衛星回線伝送路１２から受信した、平文データ１８および暗号化データ１９をＩＰデータグラム分解器２６に入力する。ＩＰデータグラム分解器２６は、受信データからＩＰヘッダ１４を分離し、この中の宛先アドレスを見て、このデータが自分宛のものか否かと、復号すべきか否かを調べる。このデータが自分宛のものである場合には、ＩＰデータグラム分解器２６はＩＰヘッダ１４を除いた受信データ２９を後段の回路、たとえば、暗号化データについては復号器９、および、平文データについては図示しない回路に送出する。復号すべき場合には、ハードウェアとして構成されている復号器９が復号鍵（復号用セッションキー）８を用いて、ＩＰヘッダ１４を分離した後の暗号化データ２９を、送信装置１における伝送すべきデータ５に相当するもとのデータ２５に復号する。衛星回線伝送路１２から受信したデータが自分宛のものであり、復号する必要のない平文である場合には、ＩＰデータグラム分解器２６はＩＰヘッダ１４を分離し、その後、復号鍵を用いて復号することなく、平文データ２８として送信装置１における伝送すべきデータ５に相当するもとの送信データを取り出す。

【００２５】図７は図５に示した受信装置２における動作処理の流れを示すフローチャートである。ステップＳ５で、受信装置２のＩＰデータグラム分解器２６は図示しない受信機（図３参照）で受信した平文データ１８および暗号化データ１９のＩＰデータグラム１５からＩＰヘッダ１４を取り出す。平文データ１８からＩＰヘッダ１４を除いてデータを平文データ２８とし、暗号化データ１９からＩＰヘッダ１４を除いてデータを暗号化データ２９とする。ステップＳ６で、信号処理装置２１はＩＰヘッダ１４の宛先アドレスを見て自分宛のデータであるかどうか判断する。自分宛のデータでない場合には受信装置２は処理を終了する。宛先アドレスが自分宛のデータである場合には、ステップＳ７に進み、信号処理装置２１はＩＰヘッダ１４を見て、暗号化データ２９を復号鍵８を用いて復号するか否かを判断する。復号鍵８を用いて暗号化データ２９を復号する場合にはステップＳ８に進み、信号処理装置２１は復号器９において復号鍵８を用いた復号処理を行なわせ、その後、ステップＳ９においてデータを取り出す。ステップＳ７において復号鍵８を用いて復号しない場合には、ステップＳ９に進み、信号処理装置２１は平文データ２８を取り出す。

【００２６】第１実施例の効果

映像・音声（ＡＶ）データ、あるいは、コンピュータデータなどの大容量のデータが衛星回線伝送路などの大容量伝送路１２を介して、必要に応じて、暗号化されて伝送される。暗号化されたＡＶデータは公衆電話回線などの小容量伝送路１３を介して事前に復号鍵８を送信装置１から送付されている受信装置２でしか有効に復号できない。したがって、図２に示した、有効に復号鍵８が授与されていない受信装置３において、仮に衛星回線伝送路１２を介して暗号化データ１９を受信したとしても意味のないデータを受信したことになり、実質的に第３者としての受信装置３（図２参照）における盗聴（盗用）

11

が防止できる。暗号鍵7に対応する復号鍵8は公衆電話回線などの衛星回線伝送路に比較して機密性の高い有線の小容量伝送路13を介して伝送されるから、盗用者が大容量伝送路12のみ監視していても、復号鍵8は判らない。したがって第3者としての受信装置3（図2参照）において衛星回線伝送路12からのデータを受信したとしても、そのデータが暗号化されていれば、有効に復号できず、事実上、盗聴されたことにならない。特に、公衆電話回線などの小容量伝送路13は送信装置1と受信装置2との間で1対1の伝送を行う有線路であるから、盗聴を意図した受信装置3（図2参照）においては接続されず、衛星回線伝送路などの大容量伝送路12に比較して、盗聴または漏洩は起こりにくい。

【0027】

【実施例2】本発明のデータ伝送装置の第2実施例を述べる。図8は本発明の第2実施例としてのデータ伝送装置の概略構成図である。図8に図解したデータ伝送装置は、1台の送信装置1に対して2台の受信装置2A，2Bがそれぞれ衛星回線伝送路などの大容量伝送路（第1の伝送系統）12および公衆電話回線などの小容量伝送路（第2の伝送系統）13を介して接続されている。受信装置3は、図2に図解した場合と同様、送信装置1とは正規に接続しない受信装置3である。大容量伝送路12および小容量伝送路13の構成は、図3に図解した構成と同様である。第2実施例においては、送信装置1から2台の受信装置2A，2Bに対して小容量伝送路13を介して復号鍵（復号用セッションキー）と、大容量伝送路12を用いる伝送において使用する宛先アドレスを伝送する。受信装置2Aに対する宛先アドレスと受信装置2Bに対する宛先アドレスとは異なる。したがって、受信装置2Aまたは2Bは自己に対する伝送か否かを宛先アドレスを検査することによって識別できる。送信装置1と受信装置2A、または、送信装置1と受信装置2Bとのデータ伝送は、それぞれ、第1実施例と同じである。第2実施例によれば、大容量伝送路12を用いて、同時に複数、本実施例は2台の受信装置2A，2Bに暗号化データを伝送し、それぞれの受信装置で復号できる。もちろん、IPヘッダ14の伝送制御情報の暗号化するか否かを示すフラグがセットされていない場合は暗号化しないデータを伝送することもできる。

【0028】第2実施例の変形例

上述した第2実施例においては、2台の独立した宛先アドレスを有する受信装置2A，2Bが、同時に大容量伝送路12を介して暗号化データを受信でき、宛先アドレスが一致する受信装置が有効に暗号化データを復号する場合について述べたが、本実施例の変形態様としては、2台の受信装置2A，2Bの宛先アドレスを同じにして、2台の受信装置2A，2Bが同時に暗号化データを受信し、2台の受信装置の両者で暗号化データを復号可能にすることもできる。このような運用の例としては、

12

たとえば、ある企業の本社から複数の支部に同じ暗号化データを伝送する場合、複数の支店ごとに伝送することなく、1度で全ての支店に伝送する場合などがある。すなわち、伝送回数を少なくできるという利点がある。また、有料映像データを暗号化して多くの有料放送加盟者に伝送する場合なども、有料放送加盟者側の受信装置の宛先アドレスを同じにしておけば、それらの複数の受信装置に暗号化された有料映像データを1度伝送するだけで、有効な受信装置側で復号できる。

【0029】

【実施例3】本発明のデータ伝送装置の第3実施例を述べる。第3実施例のデータ伝送装置の構成は、図2、図5および図8を参照して述べた第1実施例および第2実施例のデータ伝送装置の構成と同様である。ただし、第1実施例および第2実施例においては、大容量伝送路12から暗号化データを伝送する前に、送信装置1から受信装置2に復号鍵（復号用セッションキー）を小容量伝送路13を介して伝送したが、第3実施例においては、受信装置2から送信装置1に小容量伝送路13を介して事前に暗号化鍵（暗号化用セッションキー）を伝送しておく。この暗号化鍵は、受信装置2において大容量伝送路12を用いたデータ伝送において使用する受信装置2の宛先アドレスに基づいて生成される。受信装置2において、暗号鍵に対応する復号鍵は判っている。送信装置1において伝送データを暗号化する場合には、この暗号化鍵を用いて暗号化処理を行う。暗号化データ伝送およびその復号処理は、第1実施例および第2実施例と同様である。第3実施例においては、受信装置2が送信装置1に対して暗号化鍵を指定することができる。

【0030】

【実施例4】本発明のデータ伝送装置の第4実施例を述べる。図9は本発明のデータ伝送装置の第4実施例の構成図である。送信装置1と受信装置2とは大容量伝送路12と小容量伝送路13を介して接続されている。これらの接続状態は図3に図解した接続状態と同様である。送信装置1は、小容量伝送路13に接続された変復調器（モデム）17、信号処理装置11、データ暗号化器6、IPデータグラム構成器16の他、キー暗号化器130およびキー変換器132を有している。キー暗号化器130は、マスターキー120とワークキー121から暗号化したキー123を生成する。暗号化したキー123が変復調器（モデム）17を経由して受信装置2の変復調器（モデム）27で受信される。IPデータグラム構成器16は伝送すべきデータ5に、暗号化伝送データの送信先である受信装置2の宛先アドレスおよび暗号化処理を行うか否かを示すフラグを有するIPヘッダ14を付加してIPデータグラム15を構成する。IPヘッダ14の宛先アドレスは、キー変換器132に入力され、ワークキー121とともにキー変換器132において暗号鍵（暗号化セッションキー）7を生成するのに使

用される。このように、暗号鍵７は、ワークキー１２１の他に、受信装置２の宛先アドレスを元にして生成されているので、正当な受信装置２以外で暗号化伝送データを受信したとしても、正当に復号できないことになる。この詳細は後述する。キー変換器１３２で生成された暗号鍵（セッションキー）７が暗号化器６において伝送すべきデータ５を暗号化するのに使用される。暗号化器６において暗号化され大容量伝送路１２に送出されるデータが暗号化データ１９である。暗号化データ１９は、伝送すべきデータ５を暗号化したデータに、暗号化されていないＩＰヘッダ１４が付加されて、図示しない送信手段によって大容量伝送路１２に送出される。

【００３１】受信装置２は、小容量伝送路１３に接続された変復調器（モデム）２７、信号処理装置２１、ＩＰデータグラム分解器２６、データ復号器９の他に、キー復号器２３０、キー変換器２３２を有している。キー復号器２３０は変復調器（モデム）２７を経由して受信した暗号化されているキー１２３をマスターキー２２０を用いてワークキー２２１を復号する。ＩＰデータグラム分解器２６は、暗号化データ１９からＩＰヘッダ１４を分離し、受信装置２の宛先アドレスを取り出し、キー変換器２３２に印加する。キー変換器２３２は、宛先アドレスと、復号されたワークキー２２１から復号鍵（復号用セッションキー）８を変換する。本実施例においては、宛先アドレスをも用いて復号鍵８を再生しているから、正当なアドレスでない受信装置においては正当な復号鍵が生成できない。なお、本実施例における宛先アドレスは単一の装置の宛先アドレスだけを意味するだけでなく、複数の受信装置から構成されるグループを意味（指定）することができる。その場合、上述した暗号化処理および復号処理は、複数の装置に対する暗号化処理および復号処理を意味する。キー変換器２３２で変換された復号鍵８は大容量伝送路１２を経由して受信した暗号化データ１９を復号するのに使用される。

【００３２】送信装置１におけるマスターキー１２０と受信装置２におけるマスターキー２２０とは実質的に同じ内容である。マスターキー１２０を記録した物体を郵送する等して、送信装置１と受信装置２とでマスターキー１２０（２２０）を共有している。送信装置１はワークキー１２１を生成し、キー暗号化器１３０においてマスターキー１２０を鍵としてワークキー１２１を暗号化し、暗号化したキー１２３を変復調器（モデム）１７を介して小容量伝送路１３に送出し受信装置２に伝送する。また、ワークキー１２１をキー変換器１３２に入力して暗号鍵７に変換し、変換した暗号化鍵（暗号化用セッションキー）７を鍵として、データ暗号化器６において伝送すべきデータ５を暗号化して暗号化データ１９として大容量伝送路１２を介して受信装置２に伝送する。受信装置２において、小容量伝送路１３から受信した暗号化したキー１２３をキー復号器２３０においてマスターキー２２０を用いてワークキー２２１を復号し、キー変換器２３２で復号鍵８に変換し、変換された復号鍵（復号用セッションキー）８を鍵としてデータ復号器９において大容量伝送路１２から受信した暗号化データ１９を復号する。

【００３３】第４実施例のデータ伝送装置の送信装置１におけるワークキーの暗号化処理は、送信装置１と受信装置２の間で既に共有済みの受信装置２が持つ受信端末のシリアルナンバー等の固有情報を鍵（マスターキー）として行えば、受信装置２においてワークキーを得られるように行なわれる。

【００３４】第４実施例においては、暗号化したキー１２３を小容量伝送路１３を経由して伝送するから、ワークキーの漏洩があっても、マスターキー１２０を知らない限り復号鍵８が生成される可能性が殆どないので、鍵伝送の機密性が非常に高い。したがって、大容量伝送路１２を伝送された暗号化データ１９が第３者の受信装置３において正しく復号することが困難であり、情報の漏洩についても安全性がより高かまる。さらに第４実施例においては、送信先の受信装置２の宛先アドレスをも用いて暗号鍵７および復号鍵８の生成（変換）を行うので、正当な受信装置２でしか正当な暗号化器６を生成（再生）できず、かりに暗号化データ１９を受信したとしても正常に暗号化データ１９を復号できない。

【００３５】第４実施例の第１変形例

図９には、好適実施例として、送信装置１においてワークキー１２１を暗号化して暗号化したキー１２３として受信装置２に伝送する例を示したが、第４実施例は、受信装置２の宛先アドレスを用いて暗号鍵７および復号鍵８を変換していて機密性が高くなっているので、ワークキー１２１を小容量伝送路１３を経由して直接、キー変換器２３２における復号鍵（復号化セッションキー）８の変換に使用してもよい。すなわち、図９に図解した送信装置１におけるキー暗号化器１３０、受信装置２におけるキー復号器２３０を削除することができる。この場合、マスターキー１２０、マスターキー２２０の交換をしないで済むので、送信装置１と受信装置２との間の手続きは簡単になる。

【００３６】第４実施例の第２変形例

また、図９を参照して述べた第４実施例は、好適実施例として、送信装置１におけるキー変換器１３２においてワークキー１２１と宛先アドレス１４を用いて暗号化セッションキー７を変換し、その暗号化セッションキー７を用いてデータ１５を暗号化器６において暗号処理する場合を述べたが、第４実施例の簡便な例として、キー変換器１３２において、宛先アドレス１４を用いず、ワークキー１２１のみを用いて暗号化鍵（暗号化セッションキー）７を生成することができる。この場合、キー変換器１３２の構成が簡単になる。同様に、受信装置２におけるキー変換器２３２においても、マスターキー１２０

15

と同じマスターキー２２０を用いて復号鍵（復号セッションキー）８を生成して、その復号鍵８を用いて受信した暗号化データを復号できる。この場合も、キー変換器２３２の構成が簡単になる。

【００３７】第４実施例の第３変形例

さらに、上述した第４実施例の第１の変形例と第２変形例を組み合わせることもできる。すなわち、第４実施例の第１変形例に従って、図９に図解した送信装置１におけるキー暗号化器１３０、受信装置２におけるキー復号器２３０を削除し、第２変形例に従って、キー変換器１３２およびキー変換器２３２の構成を簡単にする。

【００３８】

【実施例５】本発明のデータ伝送装置の第５実施例を述べる。図１０は本発明のデータ伝送装置の第５実施例の構成図である。第４実施例においては、小容量伝送路１３を用いて、送信装置１から受信装置２に暗号化したキー１２３を伝送したが、第５実施例は、１台の受信装置２が存在しただけのとき、受信装置２から送信装置１に暗号化したワークキー２２３を小容量伝送路１３を経由して伝送し、送信装置１において、暗号化したワークキー２２３からワークキー１２１を復号し、このワークキー１２１から暗号鍵７を変換する。このため、送信装置１には、図９に図解したキー暗号化器１３０に代えてキー復号器２３０と同等のキー復号器１３４が設けられ、受信装置２には、図９に図解したキー暗号化器１３０と同等のキー暗号化器２３４が設けられている。その他の構成および動作は第４実施例と同様である。第５実施例においては、送信装置１に対して受信装置２から暗号化鍵（暗号化用セッションキー）を指定することができる。第５実施例における鍵の機密性、暗号化データ１９の機密性は第４実施例と同等である。

【００３９】第５実施例の変形例

図１０には、好適実施例として、送信装置１においてワークキー１２１を暗号化して暗号化したキー１２３として受信装置２に伝送する例を示したが、第５実施例は、第４実施例と同様、受信装置２の宛先アドレスを用いて暗号鍵７および復号鍵８を変換していて機密性が高いので、ワークキー２２１を小容量伝送路１３を経由して直接、送信装置１のキー変換器１３２における暗号鍵７の変換に使用してもよい。すなわち、送信装置１におけるキー復号器１３４、受信装置２におけるキー暗号化器２３４を削除することができる。この場合、マスターキー１２０、マスターキー２２０の交換をしないで済むので、手続きは簡単になる。その他、第５実施例についても、第４実施例の変形例として述べた種々の簡単な構成をとることができる。

【００４０】

【実施例６】本発明のデータ伝送装置の第６実施例を述べる。第４実施例および第５実施例においては、送信装置１および受信装置２において、好適には、ワークキー

16

１２１と宛先アドレスから、簡便には、第４実施例の変形例として述べたように、ワークキー１２１から暗号鍵（暗号用セッションキー）７を変換するためのキー変換器１３２、および、ワークキー２２１から復号鍵（復号用セッションキー）８を変換するためのキー変換器２３２を設けている。これに対して第６実施例においては、送信装置１のキー変換器１３２の入力を、ワークキー１２１と大容量伝送路１２を用いる伝送における宛先アドレスとし、これらの情報から暗号鍵（暗号用セッションキー）７を生成する。同様に、受信装置２のキー変換器２３２の入力を、ワークキー２２１と受信装置２のアドレスとし、これらの情報から復号鍵（復号用セッションキー）７を生成する。その他の構成および動作は第４実施例と同様である。なお、第６実施例においても、宛先アドレスは単一の装置の宛先アドレスだけを意味するだけでなく、複数の受信装置から構成されるグループを意味（指定）することができる。その場合、上述した暗号化処理および復号処理は、複数の装置に対する暗号化処理および復号処理を意味する。第６実施例においては、第４実施例のようにワークキーのみからセッションキーを生成する方法に対して、宛先アドレスを知らない者にはセッションキーを生成することが困難であるから、鍵の伝送の安全性がより高くなるという利点がある。

【００４１】

【実施例７】本発明のデータ伝送装置の第７実施例を述べる。図１１は本発明のデータ伝送装置の第７実施例の構成図である。データ伝送装置は、大容量伝送路１２および小容量伝送路１３を介して接続される送信装置１と受信装置２とを有する。送信装置１は、暗号化器６およびキー暗号化器１３６を有する。受信装置２は復号器９およびキー復号器２３６を有する。なお図解を簡単するするため、図１１には図５に示したＩＰデータグラム構成器１６およびＩＰデータグラム分解器２６は図示していない。しかしながら、本実施例においても、ＩＰヘッダ１４に規定されている宛先データの処理および暗号処理を行うか否かの処理は上述した実施例と同様に行う。

【００４２】第４実施例では送信装置１から受信装置２に暗号化したキー１２３を小容量伝送路１３を用いて伝送し、第５実施例では受信装置２から送信装置１に暗号化したワークキー２２３を小容量伝送路１３を用いて伝送している。これに対して第７実施例では、送信装置１から受信装置２に暗号化したセッションキー１２４を小容量伝送路１３を用いて伝送する。また、受信装置２が１台の場合は、受信装置２から送信装置１に暗号化したセッションキーを小容量伝送路１３を用いて伝送する。このセッションキーは、大容量伝送路１２を用いた暗号化データ伝送における宛先アドレスに基づいて生成される。

【００４３】送信装置１において暗号化用鍵（暗号化用セッションキー）７を生成し、送信装置１と受信装置２

において共有するマスターキー１２０を鍵としてキー暗号化器１３６を用いて暗号化し、暗号化されたセッションキー１２４を小容量伝送路１３を用いて受信装置２に送る。送信装置１においては、生成した暗号化鍵７を鍵として暗号化器６を用いて伝送すべきデータ５を暗号化して大容量伝送路１２を用いて受信装置２に送る。受信装置２は小容量伝送路１３から受信した暗号化されたセッションキー１２４をマスターキー２２０を鍵として復号器９で復号し、復号鍵（復号用セッションキー）８を得る。受信装置２において、大容量伝送路１２から受信した暗号化データ１９を、上記のようにして求めた復号鍵８を鍵として復号器９で復号する。第７実施例は、直接、暗号化したセッションキー１２４を送信装置１から受信装置２に伝送しているので、送信装置１および受信装置２におけるキー変換器１３２およびキー変換器２３２が不要であるという構成上の利点がある。

【００４４】

【実施例８】本発明のデータ伝送装置の第８実施例を述べる。図１２は本発明のデータ伝送装置の第８実施例の構成図である。送信装置１はＩＰデータグラム構成器１６および暗号化器６を有する。受信装置２は復号器９およびＩＰデータグラム分解器２６を有する。送信装置１において、伝送すべきデータ５がＩＰデータグラム構成器１６に入力されてＩＰヘッダ１４が付加されてＩＰデータグラム１５が形成される。暗号化器６はＩＰヘッダ１４に含まれる宛先データも暗号化する。ＩＰヘッダ１４のデータも暗号化したデータ１９が大容量伝送路１２を経由して受信装置２に伝送される。受信装置２は、大容量伝送路１２から受信したＩＰヘッダ１４のデータも暗号化したデータ１９の全てを復号器９において復号する。それにより、ＩＰデータグラム１５も復号される。ＩＰデータグラム分解器２６が復号したＩＰデータグラム１５を分解してＩＰヘッダ１４を取り出し、この中の宛先アドレスを見て、それが自分宛のデータであるか否かを知り、自分宛のデータである場合には、ＩＰヘッダを取り除いたもとのデータ部分を取り出す。なお、本実施例において、小容量伝送路１３を用いた送信装置１と受信装置２との間の暗号鍵または暗号鍵を生成するための情報の授受、あるいは、送信装置１と受信装置２との間で復号鍵または復号鍵を生成するための情報の授受は、上述した第１～第７実施例のいずれも適用できる。すなわち、本実施例は、ＩＰヘッダ１４も暗号化の対象にした例を示しており、小容量伝送路１３を用いた暗号鍵または復号鍵の伝送方法は上述した実施例のいずれも適用できる。本実施例においては、送信装置１または受信装置２において、伝送されているデータを暗号化あるいは復号するかしないかの判断を省略することができる。

【００４５】変形例

上述した実施例は全て、インターネット・プロトコルＩＰを用いた場合について例示したが、本発明の実施に際しては、インターネット・プロトコルＩＰに限定されず、その他の伝送プロトコル、たとえば、ＡＴＭ（Asynchronous Transfer Mode、非同期転送モード）に従うプロトコルなどを用いることができる。また本発明の実施に際しては、上述した種々の実施例を適宜組み合わせることができる。

【００４６】

【発明の効果】本発明によれば、データを伝送する大容量伝送路（第１の伝送系統）とは異なる小容量伝送路（第２の伝送系統）を用いて暗号化あるいは復号の処理のための鍵あるいはこの鍵を生成するための情報を伝送して鍵の伝送の機密性を高めており、大容量伝送路を介して伝送される暗号化データの漏洩に対して安全性が高くなる。特に、本発明においては、制御情報として宛先データを付加しているので、正当な受信装置（第２の伝送装置）においてのみ有効に暗号化データが復号可能となる，また本発明においては、鍵を暗号化して伝送できるので、鍵の漏洩に対する安全性が一層高まる。

【００４７】また本発明によれば、伝送のために必要な制御情報を見るだけで暗号化、復号の必要性が判別できる。

【図面の簡単な説明】

【図１】図１は伝送路上のデータを暗号化する伝送方法の一例を示す概略図である。

【図２】図２は本発明のデータ伝送装置の第１実施例の構成を示す概略図である。

【図３】図３は本発明の実施例のデータ伝送装置における大容量伝送路および小容量伝送路の具体的構成を示す図である。

【図４】図４はインターネット・プロトコルＩＰにおけるメッセージ伝送の単位であるＩＰデータグラムの概略図である。

【図５】図５は図２に図解した本発明のデータ伝送装置の第１実施例についてインターネット・プロトコルＩＰを適用して実現したより詳細な構成を示す図である。

【図６】図６は本発明のデータ伝送装置の実施例における送信装置の動作処理を示すフローチャートである。

【図７】図７は本発明のデータ伝送装置の実施例における受信装置の動作処理を示すフローチャートである。

【図８】図８は本発明のデータ伝送装置の第３実施例の概略構成図である。

【図９】図９は本発明のデータ伝送装置の第４実施例の構成図である。

【図１０】図１０は本発明のデータ伝送装置の第５実施例の構成図である。

【図１１】図１１は本発明のデータ伝送装置の第７実施例の構成図である。

【図１２】図１１は本発明のデータ伝送装置の第８実施例の構成図である。

19

【符号の説明】

１・・送信者　２・・受信者　３・・盗聴受信装置

５・・伝送すべきデータ

６・・暗号化器　７・・暗号鍵（暗号化用セッションキー）

８・・復号鍵（復号化用セッションキー）

９・・復号器

１２・・大容量伝送路（衛星回線伝送路）

１３・・小容量伝送路（公衆電話回線）

20

１４・・ＩＰヘッダ

１５・・ＩＰデータグラム

１６・・ＩＰデータグラム構成器　２６・・ＩＰデータグラム分解器

１７、２７・・変復調器（モデム）

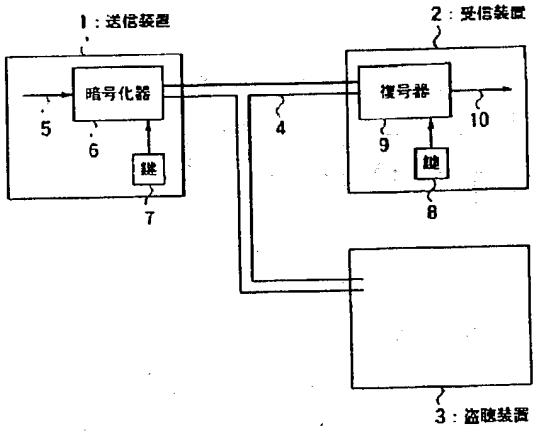
１９・・暗号化データ

１２０，２２０・・マスターキー

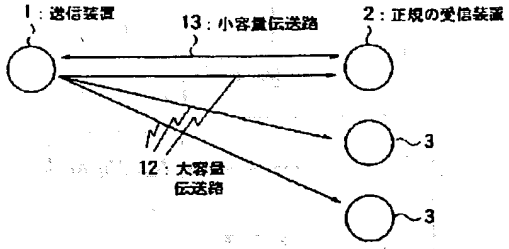
１２１，２２１・・ワークキー

１２３，２２３・・暗号化したキー

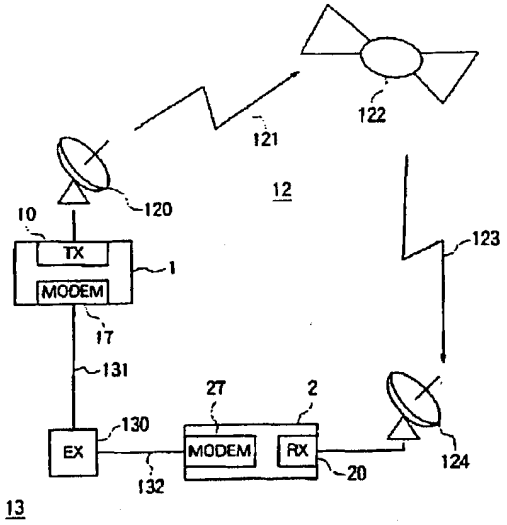
【図１】



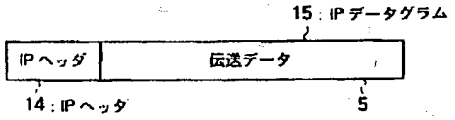
【図２】



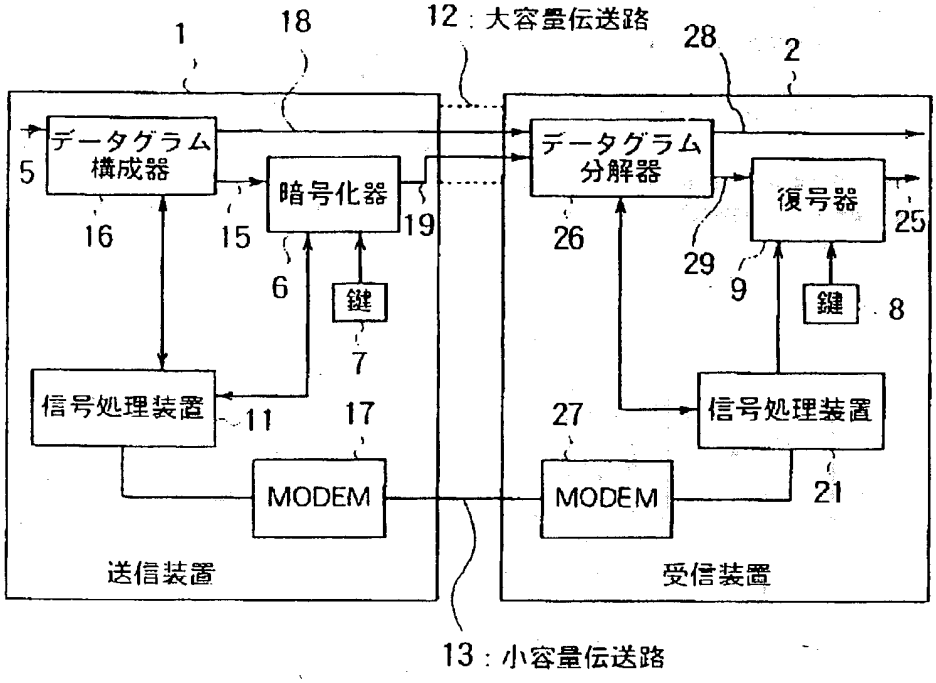
【図３】



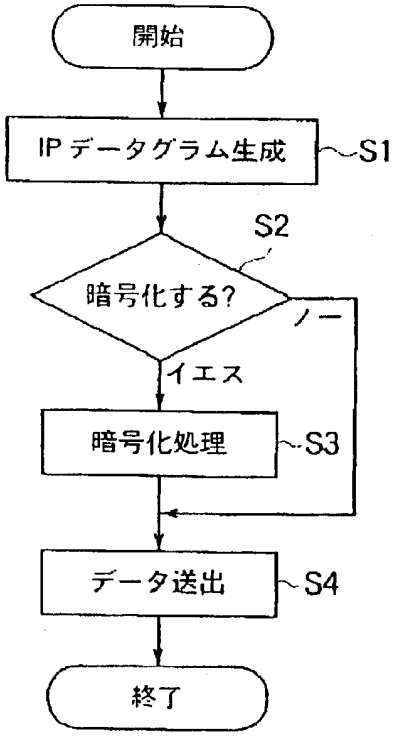
【図４】



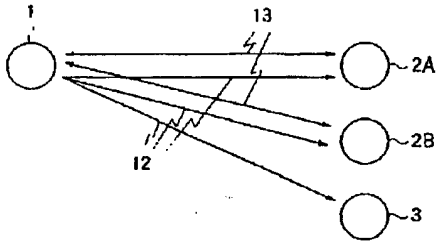
【図5】


12：大容量伝送路
1
18
28
2
データグラム
構成器
5
暗号化器
19
データグラム
分解器
復号器
25
16
15
26
29
9
6
鍵
鍵
8
7
信号処理装置
11
17
27
信号処理装置
MODEM
MODEM
21
送信装置
受信装置
13：小容量伝送路

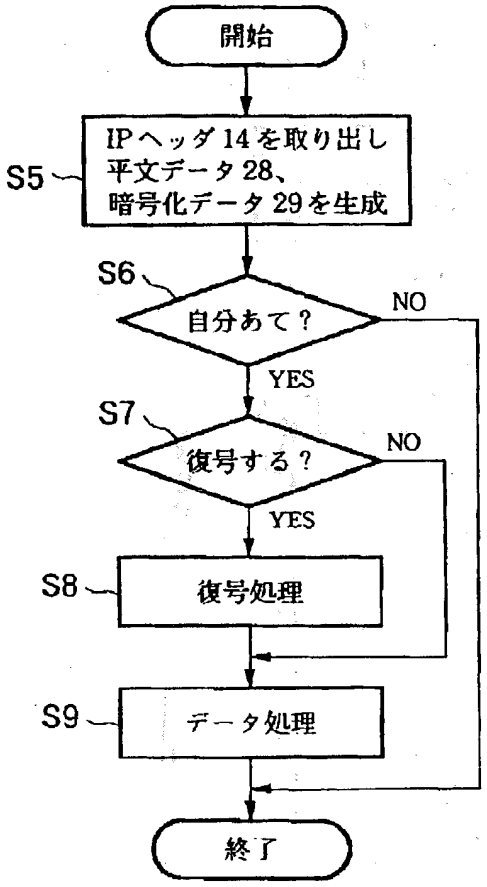
【図6】


開始
IP データグラム生成
S1
S2
暗号化する?
ノー
イエス
暗号化処理
S3
データ送出
S4
終了

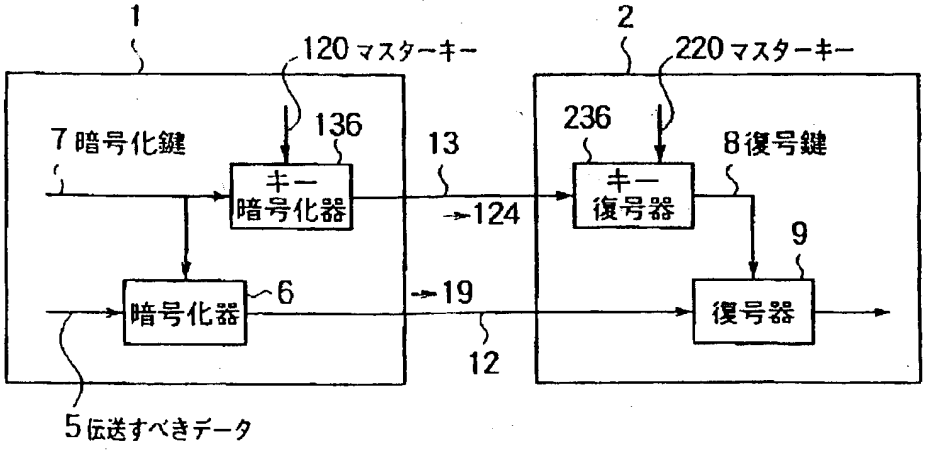
【図8】


1
13
2A
2B
12
3

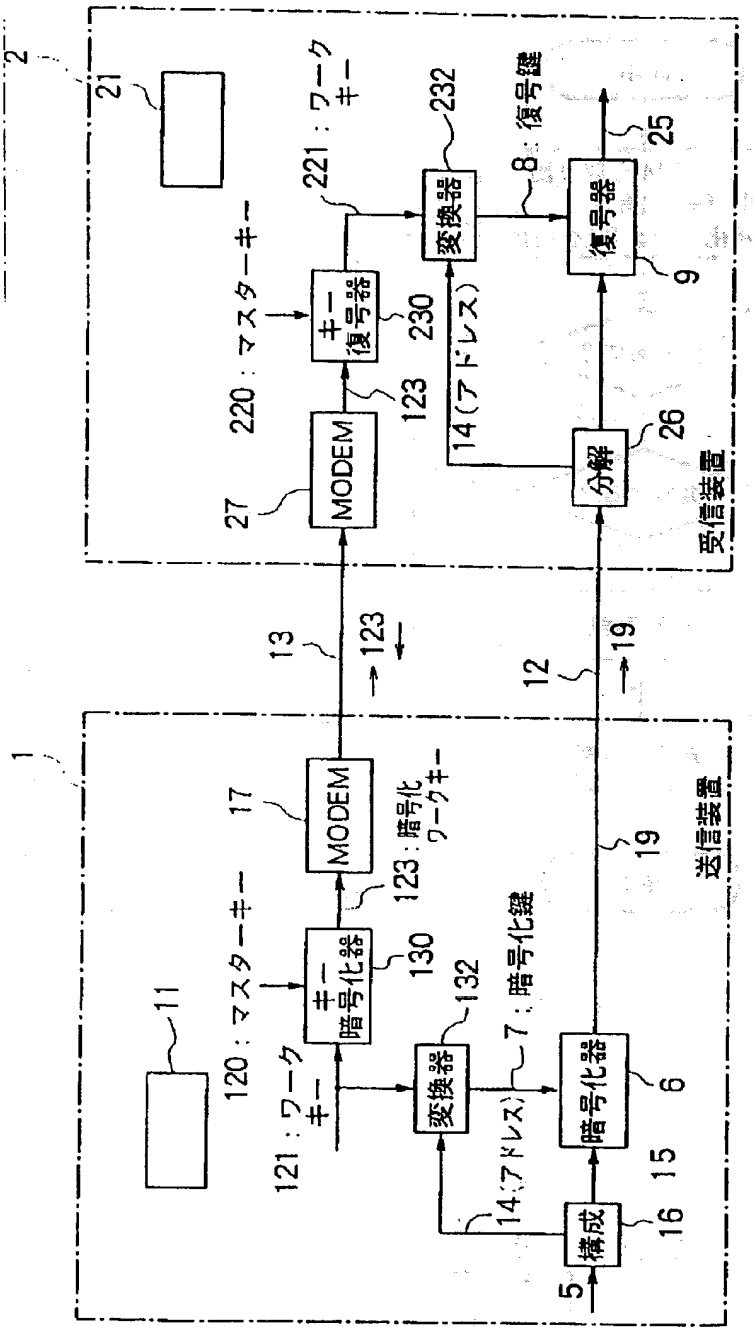
【図7】


開始
IPヘッダ14を取り出し
平文データ28、
暗号化データ29を生成
S5
S6
自分あて？
NO
YES
S7
復号する？
NO
YES
S8
復号処理
S9
データ処理
終了

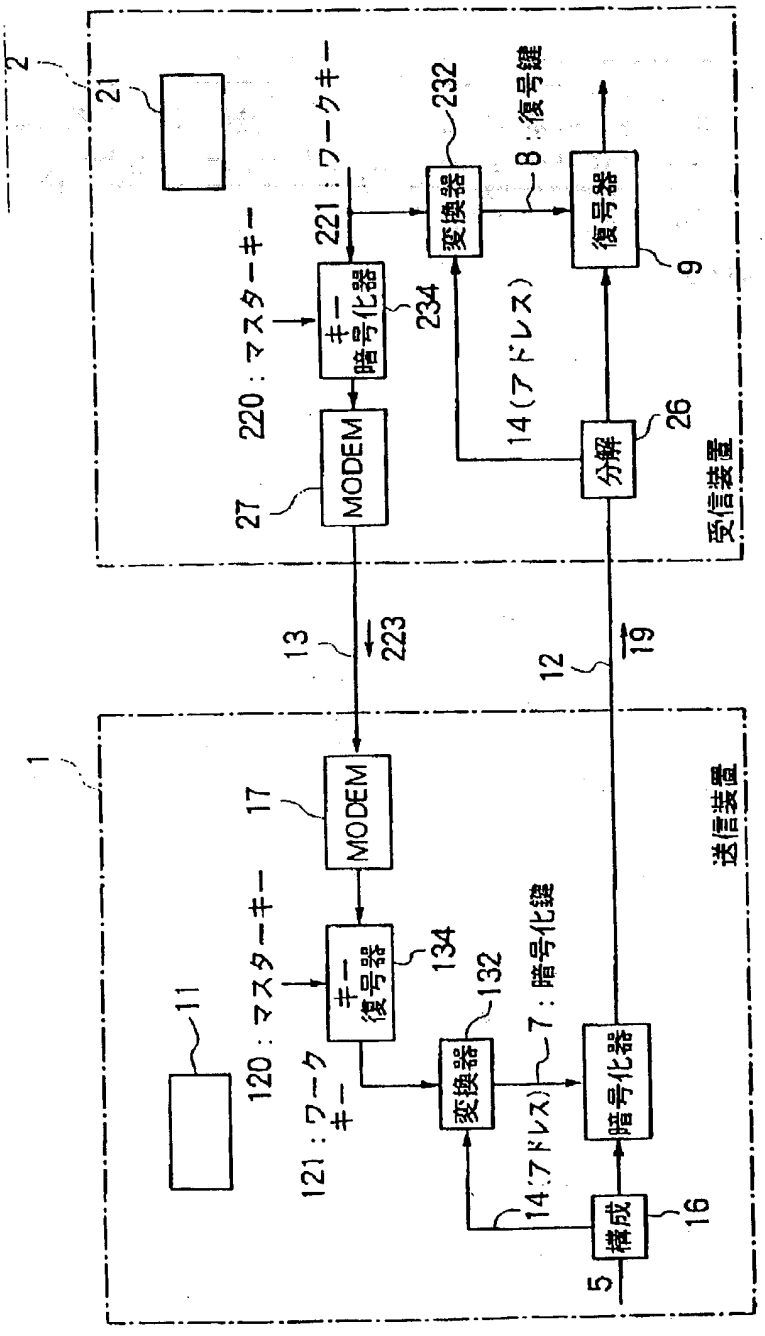
【図11】


1
120 マスターキー
2
220 マスターキー
7 暗号化鍵
136
キー
暗号化器
13
124
236
キー
復号器
8 復号鍵
9
暗号化器
6
19
復号器
12
5 伝送すべきデータ

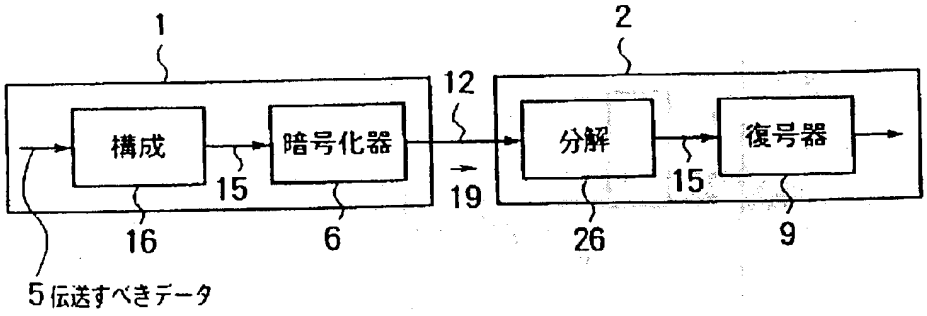
【図9】


1
送信装置
2
受信装置
5
構成
6
暗号化器
7：暗号化鍵
8：復号鍵
9
復号器
11
12
13
14（アドレス）
15
16
17
MODEM
19
120：マスターキー
121：ワークキー
123
123：暗号化ワークキー
130
キー暗号化器
132
変換器
220：マスターキー
221：ワークキー
230
キー復号器
232
変換器
25
26
分解
27
MODEM

【図１０】


2
21
232
8：復号鍵
221：ワークキー
変換器
復号器
9
キー暗号化器
234
220：マスターキー
14（アドレス）
MODEM
27
26
分解
受信装置
13
223
12
19
1
MODEM
17
送信装置
キー復号器
134
120：マスターキー
11
132
7：暗号化鍵
121：ワークキー
変換器
暗号化器
14：アドレス
構成
16
5

【図１２】



JP 9-307542

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 833 294 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
01.04.1998 Bulletin 1998/14

(21) Application number: **97907342.6**

(22) Date of filing: **17.03.1997**

(51) Int. Cl.[6]: **G09C 1/00**, H04L 9/00

(86) International application number:
PCT/JP97/00850

(87) International publication number:
WO 97/34279 (18.09.1997 Gazette 1997/40)

(84) Designated Contracting States:
DE FR GB

(30) Priority: **15.03.1996 JP 59745/96**
15.03.1996 JP 59746/96
14.06.1996 JP 154688/96

(71) Applicant: **SONY CORPORATION**
Tokyo (JP)

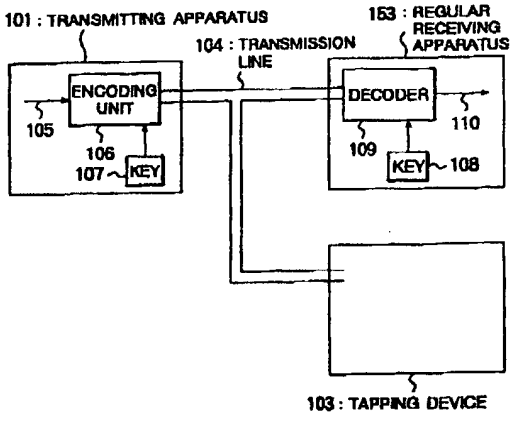
(72) Inventors:
- **ASANO, Tomoyuki**
  Shinagawa-ku, Tokyo 141 (JP)
- **ISHII, Makoto**
  Shinagawa-ku, Tokyo 141 (JP)
- **KUBOTA, Ichiro**
  Shinagawa-ku, Tokyo 141 (JP)

(74) Representative:
Körber, Wolfhart, Dr. rer.nat.
Patentanwälte
Mitscherlich & Partner,
Sonnenstrasse 33
80331 München (DE)

(54) DATA TRANSMITTER, DATA TRANSMISSION METHOD, DATA RECEIVER, DATA RECEIVING METHOD, DATA TRANSFER DEVICE, AND DATA TRANSFER METHOD

(57) The present invention provides a data transmission apparatus which enhances the safety with respect to leakage of encoded transmitted data by raising the safety of transmission of an encoding key or a decoding key. It provides a large capacity transmission line 152 such as a satellite transmission line for transmitting a large amount of data and a small capacity transmission line 156 such as a public telephone line for transmitting an encoding key or decoding key or information for the generation of them. The encoding session key 107 is generated by using a work key and a destination address of a receiving apparatus of the destination. Further, the decoding session key 108 is generated using one's own address and the work key. The work key is preferably encoded and transmitted through the small capacity transmission line 156. In the transmitting apparatus 101, in addition to the encoding of the data 105 which should be transmitted by using the encoding session converted as described above, transmission control information such as destination data is added and is transmitted to the receiving apparatus 102 through the large capacity transmission line 152. In the receiving apparatus 102, the encoded data 110 is decoded by using the decoding session key 108 converted as described above.

FIG. 1



EP 0 833 294 A1

Description

TECHNICAL FIELD

The present invention relates to a data transmission apparatus for transmitting data and a method of the same, more particularly relates to a data transmission apparatus which suitably manages an encoding key and a decoding key used where a large amount of data is encoded and transferred and a method of the same.

BACKGROUND ART

Conventionally, in a TV broadcast or other data distribution service using a communications satellite, the flow of data was made in only one direction, that is, from the data distributer to the user. In recent years, since the transmission of digital data using communications satellite has becomes possible, transmission using the communications satellites has started for not only analog video and audio data such as TVS and movies, but also the text utilized in computers and digital video and audio data.

Here, conventional data distribution services using communications satellites such as TV broadcasting has been of the form with data distributed by a data distributor being simultaneously received and used by a large number of users. Contrary to this, where the digital data used in computers is distributed via a communications satellite, a function for distributing the data from the data distributor to a single or a plurality of users is required.

In the conventional transmission system using a communications satellite, however, there is a problem in that since the distribution is performed for analog data and since the data distribution is performed in only one direction from the data distributor to the user, no function for checking the errors in transmission is provided, so the reliability of the data transmission is low. In the distribution of digital data, if even one bit of error is caused in the data due by the transmission, the received data no longer has any meaning.

In order to distribute such digital computer data by a wireless system with a high quality, it is necessary to secure a communication path for not only the distribution of data in one direction from the data distributor to the user, but also a communication path from the user to the data distributor, but the conventional transmission system is not provided with such a function.

Also, in the conventional simultaneous communication or broadcast system from a data distributor to many users, all users always receive, use, or view the same information and there is no personal identification information of the system users, therefore there is a problem that it is not possible to distribute data from the data distributor to only specific users.

Further, where data is transmitted or a conversation is conducted by using a public telephone line, dedicated line, etc., in order to prevent the leakage of the transmitted information or maintain the reliability of the information against attack (interference) with respect to the transmitted information, plain text data is encoded (scrambled) and then transmitted, and the encoded data is decoded (descrambled) at the destination of reception. As a typical encoding system, a common key encoding system and a public key system have been known.

The common key encoding system is also referred to as the symmetrical encoding system. An algorithm private type and an algorithm public type have been known. As a typical algorithm public type, the DES (data encryption standard) has been known.

In the public key system, since an enormous amount of calculation is necessary for deriving the generated key from an inspection key, the generated key is not substantially decoded, therefore it is an encoding system wherein the encoding key can be made public and is referred to also as the asymmetrical key encoding system.

The encoding system is determined in accordance with the type of the line system through which the transmission data is transmitted, the degree of secrecy (secret) of the transmitted data, the amount of transmitted data, etc.

In data transmission using a dedicated line, the degree of leakage of the information and the attack to the transmitted data is low, but when data is transmitted by using a public telephone line, the degree of the leakage of information and the degree of attack become high. Further, the transmission of data using a satellite broadcasting line can be received by many unspecified apparatuses, therefore the degree of leakage of information becomes further higher.

Figure 1 is a schematic structural view of an example of an encoded data transmitting apparatus for encoding the data on the transmission line by a common key encoding system.

In the encoded data transmitting apparatus of Fig. 1, reference numeral 101 denotes a transmitting apparatus (transmitter), reference numeral 102 denotes a receiving apparatus (receiver), 103 denotes a tapping apparatus (tapper), reference numeral 104 denotes a data transmission line, reference numeral 105 denotes data which should be transmitted, reference numeral 106 denotes an encoding unit provided in the transmitting apparatus 101, reference numeral 107 denotes an encoding key (encoding session key) used for the encoding in the encoding unit 106, reference numeral 108 denotes a decoding key (decoding session key), reference numeral 109 denotes a decoder for decoding the encoded data received from the data transmission line 104 using the decoding key, and reference numeral 110 denotes the data after decoding.

The transmitting apparatus 101, when transmitting the data 105 onto the transmission line 104, has the encoding unit 106 encode the data 105 by using the encoding key 107 and transmits the encoded data to the

receiving apparatus 102 via the transmission line 104.

The receiving apparatus 102, when receiving the encoded data from the transmission line 104 (encoded data), has the decoder 109 decode the received encoded data by using the decoding key 108 corresponding to the encoding key 107 so as to obtain an intended decoded (deciphered) data 110.

In this example, even if the tapping apparatus 103 receives the encoded data from the transmission line 104 in the same way as the receiving apparatus 102, there is no decoding key 108, so it is difficult to correctly decode this. Namely, the tapping apparatus 108 ends up handling encoded (scrambled) data as is, therefore, in actuality, the information is prevented from being leaked to the tapping apparatus 103 side.

In a principal encoding system of the common key encoding system in this example, generally the encoding key 107 and the decoding key 108 have the same bit train.

Recently, broadcasters have been making satellite broadcasts for providing TV programs to only specific contractors. The transmission system used for the satellite broadcast can transmit a large amount of data (information) such as a video and audio in a short time. Further, a transmission system using a satellite can transmit a large amount of information in a short time and therefore is not limited to broadcasts - it has been widely utilized for the transmission of data such as computer data.

In transmission using a satellite, however, unlike a one-to-one communication system such as a telephone line and dedicated line, many unspecified receivers can easily receive the data (by receiving apparatuses), so it is easy to be tapped by nature. As a result, there is a high possibility that for example a pay satellite broadcast will be tapped. Therefore, it has been proposed too to also encode the video data and audio data of a TV broadcast for transmission.

In actual transmission, the encoding is not carried out for all data, but the data which should be encoded is encoded and transmitted onto the transmission line in accordance with the content of the data to be transmitted in the transmitting apparatus (for example, whether it is pay data or not). The receiver decodes all or part of the encoded data to determine whether or not the all or partially decoded data is necessary for it at the present by the information obtained as a result of this.

In the encoded data transmitting apparatus for transmitting encoded data in this way, it is necessary for the transmission side and reception side to hold the encoding key and decoding key in advance in secret so as not to be known to third parties.

As the conventional method wherein the transmission side holds the encoding key and the reception side holds the decoding key, for example, when encoding and transmitting video data etc. by using for example a satellite transmission line, consideration may be made of the method of the transmitter sending the receiver a piece of paper, an IC card, etc. on which the decoding key is recorded by the mail or another method, the method of transmitting the encoding key and the decoding key through the same transmission line as the satellite transmission line for sending the video data (satellite transmission line), and further a method combining them.

In the conventional method of management of an encoding keg and decoding key, there are the following problems.

A first problem is the problem related to how the transmitter gets to hold the encoding key or the problem related to how the receiver gets to hold the decoding key or the problem related to how the receiver gets to hold the decoding key.

As explained above, as the method for having the encoding key held by the transmitter and having the decoding key held by the receiver, the method for sending an object such as the paper and IC card on which the decoding key is recorded from the transmitter to the receiver by the method of mail, etc., the method of sending the same by the satellite transmission line, and further the method combining them are general.

(1) In the method of sending an object on which the decoding key is recorded through the mail etc., due to the trouble of the procedure thereof, it is not easy to change the encoding key and the decoding key. This means that a large amount of data encoded using the same key will be transmitted onto the transmission line and that, since a large amount of information will be given to the tapper, the safety with respect to the deciphering will be low.

(2) In the method of sending the decoding key by using a satellite transmission line, the data on the satellite transmission line will be received by many unspecified persons having the antennas and other equipment irrespective of whether or not the transmitter desires these persons as the receivers, so there is a possibility that the decoding key will be learned by persons other than the receivers expected by the transmitter and therefore there is problem that the safety of the transmission cannot be held.

(3) In the method combining the above two methods, that is, the method of preparing the decoding key from information recorded on an object sent by mail etc. and information transmitted through a satellite transmission line, the drawbacks of the two methods are compensated and the safeness of the transmission method becomes higher to a certain extent. However, the problem that information for a decoding key sent through the mail etc. cannot be easily changed due to the troublesomeness of the procedures and the problem that the information for a decoding key transmitted through a satellite transmission line ends up being received by a large number of unspecified persons not desired by the

transmitter remain.

A second problem relates to how to decide whether or not the transmitter has encoded the data or how the receiver should decode the received data.

As mentioned above, in the methods which are used in general at the present, the transmitting apparatus views the contents of the data, encodes the data which must be encoded, and transmits it onto the transmission line. The receiving apparatus decides whether or not this data is necessary for itself by the information obtained by decoding all or part of the encoded data received from the transmission line. In this method, however, the transmitting apparatus has to perform processing for learning the contents of the data for determining whether or not the data must be encoded. Further, the receiving apparatus has to determine whether the received encoded data is required by it or not, that is, has to perform processing for decoding all or part of the encoded data for deciding whether or not the data is addressed to itself. For this reason, while it is necessary to perform the transmission at a higher speed and perform the processing in the apparatuses, with the hardware configuration heretofore, such a demand could not be satisfied.

DISCLOSURE OF THE INVENTION

An object of the present invention is to enable effective encoding of transmitted data at the transmitting side and effective decoding of the encoded data transmitted at the receiving side.

Another object of the present invention is to enable transmission of digital data by a wireless method without causing errors in transmission.

Still another object of the present invention is to enable transmission of digital data by a wireless method from a transmitting apparatus to just specific clients.

According to the present invention, there is provided a data transmitting apparatus connected to a first transmission system and a second transmission system, the data transmitting apparatus having a key transmitting means for transmitting through the second transmission system decoding key information for decoding encoded data sent through the first transmission system, generating means for adding first transmission control information to the data to be encoded and transmitted so as to generate transmitted data, encoding means for generating encoded data from the transmitted data based on encoding key information corresponding to the decoding key information, and data transmitting means for transmitting to the first transmission system the encoded data generated by the encoding means.

Preferably, the communication capacity per unit time of the first transmission system is larger than the communication capacity per unit time of the second transmission system. Specifically, the first transmission system includes a satellite transmission line and the second transmission system includes a cable transmission line.

Preferably, the key transmitting means transmits destination information of the transmitted data along with the decoding key information through the second transmission system.

More preferably, the key transmitting means transmits the same decoding key information and destination information to a plurality of receiving apparatuses connected to the first transmission line and the second transmission line.

Still more preferably, the encoding means generates encoded data from the transmitted data based on the encoding key information and the destination information of the transmitted data.

Preferably, further provision is made of a key encoding means for encoding the work key information to generate decoding key information.

Preferably, the encoding means generates encoded data from the transmitted data based on the work key information and the destination information of the transmitted data.

Preferably, the first transmission control information includes the destination information of the transmitted data.

Preferably, the first transmission control information includes an address defined by an Internet protocol as the destination information.

Preferably, the encoding means encodes the transmitted data including the first transmission control information.

Preferably, the encoding means adds to the transmitted data second transmission control information including the same destination information as the destination information included in the first transmission control information to generate the encoded data.

Preferably, the encoding means adds a CRC check bit to generate the encoded data.

Preferably, the second transmission control information includes information indicating the presence of coding of the data to be transmitted.

Preferably, the second transmission control information includes information for distinguishing whether the data to be transmitted is information responding to a request from a receiving apparatus or whether it is control information for operating the communications system including the data transmitting apparatus.

Further, according to the present invention, there is provided a data transmitting apparatus connected to a first transmission system and a second transmission system, the data transmitting apparatus provided with a key receiving means for receiving from the second transmission system encoding key information for encoding encoded data transmitted through the first transmission system, data generating means for adding control information to the data to be encoded and transmitted to generate transmitted data, encoding means for

generating encoded data from the transmitted data based on the encoding key information, and data transmitting means for transmitting through the first transmission system the encoded data generated by the encoding means.

Preferably, the encoding means is provided with key decoding means for decoding the encoding key information to generate work key information and uses the work key information decoded by the key decoding means to generate encoded data.

More preferably, the encoding means generates encoded data based on the work key information and the destination information of the encoded data.

Further, according to the present invention, there is provided a data transmission method for transmitting data using a first transmission system and a second transmission system, the data transmission method comprising a key transmitting step for transmitting through the second transmission system decoding key information for decoding encoded data transmitted through the first transmission system, a data generating step for adding first transmission control information to the data to be encoded and transmitted to generate transmitted data, an encoding step for generating encoded data from the generate transmitted data based on encoding key information corresponding to the decoding key information, and a data transmitting step for transmitting the encoded data generated by the encoding step through the first transmission system.

Preferably, the key transmitting step transmits destination information of the transmitted data along with the decoding key information through the second transmission system.

More preferably, the key transmitting step transmits the same decoding key information and destination information to a plurality of receiving apparatuses connected to the first transmission line and the second transmission line.

Still more preferably, the encoding step generates encoded data from the transmitted data based on the encoding key information and the destination information of the transmitted data.

Preferably, further provision is made of a key encoding step for encoding the work key information to generate decoding key information.

Preferably the encoding step generates encoded data from the transmitted data based on the work key information and the destination information of the transmitted data.

Preferably, the first transmission control information includes the destination information of the transmitted data.

Preferably, the first transmission control information includes an address defined by an Internet protocol as the destination information.

Preferably, the encoding step encodes the transmitted data including the first transmission control information.

Preferably, the encoding step adds to the transmitted data second transmission control information including the same destination information as the destination information included in the first transmission control information to generate the encoded data.

Preferably, the encoding step adds a CRC check bit to generate the encoded data.

Preferably, the second transmission control information includes information indicating the presence of coding of the data to be transmitted.

Preferably, the second transmission control information includes information for distinguishing whether the data to be transmitted is information responding to a request from a receiving apparatus or whether it is control information for operating the communications system including the data transmitting apparatus.

Further, according to the present invention, there is provided a data transmission method in a transmitting apparatus connected to a first transmission system and a second transmission system, the data transmission method comprising a key receiving step for receiving from the second transmission system encoding key information for encoding encoded data transmitted through the first transmission system, data generating step for adding control information to the data to be encoded and transmitted to generate transmitted data, an encoding step for generating encoded data from the transmitted data based on the encoding key information, and a data transmitting step for transmitting through the first transmission system the encoded data generated by the encoding step.

Preferably, the encoding step is provided with a key decoding step for decoding the encoding key information to generate work key information and uses the work key information decoded by the key decoding step to generate encoded data.

More preferably, the encoding step generates encoded data based on the work key information and the destination information of the encoded data.

Further, according to the present invention, there is provided a data receiving apparatus connected to a first transmission system over which encoded data is transmitted and a second transmission system over which key information is transmitted, the data receiving apparatus provided with key receiving means for receiving from the second transmission system decoding key information for decoding encoded data received from the first transmission system, a data receiving means for receiving the decoded data from the first transmission system, a data restoring means for deleting first transmission control information from the encoded data, and a decoding means for decoding the encoded data from which the first transmission control information was deleted based on the decoding key information to generate decoded data.

Preferably, the communication capacity per unit time of the first transmission system is larger than the communication capacity per unit time of the second

transmission system. Specifically, the first transmission system includes a satellite transmission line and the second transmission system includes a cable transmission line.

Preferably, the key receiving means receives destination information of the encoded data along with the decoding key information from the second transmission system.

More preferably, a plurality of receiving apparatuses are connected to the first transmission system, and the key receiving means receives the same decoding key information and destination information as other receiving apparatuses connected to the first transmission line and the second transmission line.

Preferably, the decoding means generates decoded data from the received data based on the decoding key information and the destination information of the encoded data.

Preferably, the decoding means is provided with key decoding means for decoding the decoding key information to generate work key information and uses the work key information generated by the key decoding means to decode the encoded data.

Preferably, the decoding means decodes the encoded data based on the work key information and the destination information of the encoded data.

More preferably, the first transmission control information includes the destination information of the encoded data.

Still more preferably, the first transmission control information includes an address defined by an Internet protocol as the destination information.

Specifically, the decoding means decodes the encoded data which was encoded including the first transmission control information.

Preferably, further provision is made of a judgement means for judging if the encoded data is directed to itself based on the second transmission control information including the same destination information as the destination information included in the first transmission control information of the encoded data.

Preferably, the judgement means judges if the encoded data is directed to itself and checks to the CRC check bit added to the encoded data to check for errors.

More preferably, the judgement means judges if the encoded data is directed to itself and decides whether to decode or not based on the information indicating the presence of encoding included in the second transmission control information.

Preferably, the second transmission control information includes information for distinguishing whether the received data is information responding to a request from its own receiving apparatus or whether it is control information for operating the communications system including the receiving apparatus.

Further, according to the present invention, there is provided a data receiving apparatus connected to a first transmission system and a second transmission system, the data receiving apparatus provided with a key transmitting means for transmitting through the second transmission system encoding key information for preparing encoded data received from the first transmission system, data receiving means for receiving the encoded data encoded based on the encoding key information from the first transmission system, data restoring means for deleting the first transmission control information from the encoded data, and a decoding means for decoding the encoded data based on decoding key information corresponding to the encoding key information.

Preferably, further provision is made of a key encoding means for encoding work key information to generate encoding key information.

More preferably, the decoding means is provided with a decoding key generating means for generating a decoding key based on the work key information and the destination information of the encoded data and decodes the encoded data based on the decoding key generated by the decoding key generating means.

Further, according to the present invention, there is provided a data receiving method in a receiving apparatus connected to a first transmission system and a second transmission system, the data receiving method comprising a key receiving step for receiving from the second transmission system decoding key information for decoding encoded data received from the first transmission system, a data receiving step for receiving the decoded data from the first transmission system, a data restoring step for deleting first transmission control information from the encoded data, and a decoding step for decoding the encoded data from which the first transmission control information was deleted based on the decoding key information to generate decoded data.

Preferably, the key receiving step receives the same decoding key information and destination information as other receiving apparatuses connected to the first transmission system end the second transmission system.

More preferably, the decoding step generates decoded data from the encoded data based on the decoding key information and the destination information of the encoded data.

More preferably, the decoding step is provided with key decoding step for decoding the decoding key information to generate work key information and uses the work key information generated by the key decoding step to decode the encoded data.

Preferably, the decoding step decodes the encoded data based on the work key information and the destination information of the encoded data.

Preferably, the first transmission control information includes the destination information of the encoded data.

More preferably, the first transmission control information includes an address defined by an Internet protocol as the destination information.

Preferably, the decoding step decodes the encoded data which was encoded including the first transmission control information.

Preferably, further provision is made of a judgement step for judging if the encoded data is directed to itself based on the second transmission control information including the same destination information as the destination information included in the first transmission control information of the encoded data.

Preferably, the judgement step judges if the encoded data is directed to itself and checks to the CRC check bit added to the encoded data to check for errors.

More preferably, the judgement step judges if the encoded data is directed to itself and decides whether to decode or not based on the information indicating the presence of encoding included in the second transmission control information.

Preferably, the second transmission control information includes information for distinguishing whether the received data is information responding to a request from its own receiving apparatus or whether it is control information for operating the communications system including the receiving apparatus.

Further, according to the present invention, there is provided a data receiving method in a receiving apparatus connected to a first transmission system and a second transmission system, the data receiving method comprising a key transmitting step for transmitting through the second transmission system encoding key information for preparing encoded data received from the first transmission system, a data receiving step for receiving the encoded data encoded based on the encoding key information from the first transmission system, a data restoring step for deleting the first transmission control information from the encoded data, and a decoding step for decoding the encoded data based on decoding key information corresponding to the encoding key information.

Preferably, further provision is made of a key encoding step for encoding work key information to generate encoding key information.

Preferably, the decoding step is provided with a decoding key generating step for generating decoding key information based on the work key information and the destination information of the encoded data and decodes the encoded data based on the decoding key generated by the decoding key generating step.

Further, according to the present invention, there is provided a data transmission apparatus having a first transmission system and a second transmission system, the data transmission apparatus provided with:

a transmitting apparatus having a key transmitting means for transmitting through the second transmission system decoding key information for decoding the encoded data transmitted through the first transmission system, data generating means for generating transmitted data added with first transmission control information from the data to be encoded and transmitted, encoding means for generating encoded data from the transmitted data based on encoding key information corresponding to the decoding key information, and data transmitting means for transmitting through the first transmission system the encoded data generated by the encoding means and

a receiving apparatus having a key receiving means for receiving from the second transmission system decoding key information for decoding the encoded data received from the first transmission system, data receiving means for receiving the encoded data from the first transmission system, data restoring means for deleting first transmission control information from the encoded data, and decoding means for decoding the encoded data based on the decoding key information.

Further, according to the present invention, there is provided a data transmission apparatus having a first transmission system and a second transmission system, the data transmission apparatus provided with:

a transmitting apparatus having a key receiving means for receiving from the second transmission system encoding key information for encoding the encoded data transmitted through the first transmission system, data generating means for generating transmitted data added with control information from the data to be encoded and transmitted, encoding means for generating encoded data from the transmitted data based on encoding key information, and data transmitting means for transmitting through the first transmission system the encoded data generated by the encoding means and

a receiving apparatus having a key transmitting means for transmitting through the second transmission system encoding key information for preparing the encoded data received from the first transmission system, data receiving means for receiving the encoded data encoded based on the encoding key information from the first transmission system, data restoring means for deleting first transmission control information from the encoded data, and decoding means for decoding the encoded data based on decoding key information corresponding to the encoding key information.

Further, according to the present invention there is provided

a data transmission method using a transmission apparatus having a first transmission system and a second transmission system, the data transmission method comprising:

a transmitting processing step having a key transmitting step for transmitting through the second transmission system decoding key information for decoding the encoded data transmitted through the first transmission system, a data generating step for generating transmitted data added with first transmission control information from the data to be encoded and transmitted, an encoding step for generating encoded data from the transmitted data based on encoding key information corresponding to the decoding key information, and a data transmitting step for transmitting through the first transmission system the encoded data generated by the encoding step and

a receiving processing step having a key receiving step for receiving from the second transmission system decoding key information for decoding the encoded data received from the first transmission system, a data receiving step for receiving the encoded data from the first transmission system, a data restoring step for deleting first transmission control information from the encoded data, and a decoding step for decoding the encoded data based on the decoding key information.

Further, according to the present invention, there is provided a data transmission method for transmission of data using a transmission apparatus having a first transmission system and a second transmission system, the data transmission method comprising:

a transmitting processing step having a key receiving step for receiving from the second transmission system encoding key information for encoding the encoded data transmitted through the first transmission system, a data generating step for generating transmitted data added with control information from the data to be encoded and transmitted, an encoding step for generating encoded data from the transmitted data based on encoding key information, and a data transmitting step for transmitting through the first transmission system the encoded data generated by the encoding step and

a receiving processing step having a key transmitting step for transmitting through the second transmission system encoding key information for preparing the encoded data received from the first transmission system, a data receiving step for receiving the encoded data encoded based on the encoding key information from the first transmission system, a data restoring step for deleting first transmission control information from the encoded data, and a decoding step for decoding the encoded data based on decoding key information corresponding to the encoding key information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic view showing an example of a transmitting method for encoding data on the transmission line.

Fig. 2 is a schematic view showing the configuration of a data transmission apparatus of the present invention.

Fig. 3 is a view of an example of the configuration of a data transmission apparatus according to an embodiment of the present invention.

Fig. 4 is a view for explaining the configuration of a data transmitting apparatus shown in Fig. 3.

Fig. 5 is a view for explaining the configuration of a data receiving apparatus shown in Fig. 3.

Fig. 6 is a view for explaining the configuration of a data preparing unit shown in Fig. 4.

Fig. 7 is a view for explaining the processing in the data transmitting apparatus and data receiving apparatus.

Fig. 8 is a view for explaining a format of an IP packet.

Fig. 9 is a view for explaining the format of a MAC frame.

Fig. 10 is a view for explaining the format of a section header.

Fig. 11 is a view for explaining a packet header of a transport packet.

Fig. 12 is a view of the configuration of a first embodiment of an IP packet preparation unit and encoding unit shown in Fig. 6.

Fig. 13 is a flowchart of the operational processing of the data transmitting apparatus;

Fig. 14 is a view of the configuration of a first embodiment of a data decomposing unit shown in Fig. 5.

Fig. 15 is a flowchart of the operating processing of a data receiving apparatus.

Fig. 16 is a schematic view of the configuration of a second embodiment of a data transmission apparatus of the present invention.

Fig. 17 is a view of the configuration of a fourth embodiment of an IP packet preparation unit and encoding unit shown in Fig. 6.

Fig. 18 is a view of the configuration of a fourth embodiment of the data decomposing unit shown in Fig. 5.

Fig. 19 is a view of the configuration of a fifth embodiment of an IP packet preparation unit and encoding unit shown in Fig. 6.

Fig. 20 is the configuration of a fifth embodiment of the data decomposing unit shown in Fig. 5.

Fig. 21 is a view of the configuration of a seventh embodiment of an IP packet preparation unit and encoding unit shown in Fig. 6.

Fig. 22 is a view of the configuration of a seventh embodiment of the data decomposing unit shown in Fig. 5.

Fig. 23 is a view of the configuration of an eighth embodiment of an IP packet preparation unit and encoding unit shown in Fig. 6.

Fig. 24 is a view of the configuration of an eighth embodiment of the data decomposing unit shown in Fig. 5.

BEST MODE FOR CARRYING OUT THE INVENTION

The embodiments of the present invention will be explained below with reference to the drawings.

Fig. 2 is a conceptual view of the configuration of a data transmitting apparatus of the present invention. In Fig. 2, reference numeral 151 denotes a transmitting apparatus (transmitter), reference numeral 153 denotes a receiving apparatus (receiver), reference numeral 154 and reference numeral 155 denote receiving apparatuses of third persons other than the receiving apparatus 153, reference numeral 152 denotes a large capacity transmission line serving as the first transmission system, and reference numeral 156 denotes a small capacity transmission line serving as the second transmission system.

In the present invention, a large amount of data such as a TV signal, computer data, etc. is transmitted via the large capacity transmission line 152. As the large capacity transmission line 152, a satellite transmission line which transmits a large amount of data at a high speed and with a high efficiency is preferred.

Further, as the small capacity transmission line 156 which transmits the information concerning the encoding or decoding, a cable transmission line, for example, a public telephone line, ISDN (integrated services digital network) line, or dedicated line, which performs one-to-one communication with which the leakage of the information is smaller than a satellite transmission line is desirable.

The communication capacity per unit time of the large capacity transmission line 152 serving as the second transmission system is larger than the communication capacity per unit time of the small capacity transmission line 156 serving as the first transmission system.

Figure 3 is a schematic view of a data transmission apparatus for realizing a data service for distributing multimedia digital data (video, audio, text, etc.) Fig. 3 is a schematic view of the configuration of a transmission line using a satellite transmission line as the large capacity transmission line 152 and using a public telephone line as the small capacity transmission line 156.

A data transmitting side, that is, a data provider A, has a data transmitting apparatus 201 serving as the server, and the user B has a data receiving apparatus 203 serving as the client. Here, the data transmitting apparatus 201 and the data receiving apparatus 203 correspond to the transmitting apparatus 151 and receiving apparatus 153 in Fig. 2.

The data transmitting apparatus 201 and the data receiving apparatus 203 can communicate with each other via a public telephone line 204 capable of performing bidirectional communication and corresponding to the small capacity transmission line 156 in Fig. 2. Also, large capacity communication is possible by a wireless system from the data transmitting apparatus 201 to the data receiving apparatus 203 via a communications satellite 202 and wireless communications line 205 corresponding to the large capacity transmission line 152 in Fig. 2.

An explanation will be made next of the flow of the data in the data transmission apparatus shown in Fig. 3.

Assume that the data provider A and the user B conclude a contract for delivery of digital data in advance. At this time, assume that the data receiving apparatus 203 of the user B is provided with a function capable of receiving data from the data transmitting apparatus 201 of the data provider A.

First, the user B sends a request 212 to the data provider A via the public telephone line 204 serving as the ground communication net to the effect of wanting to receive a predetermined service provided by the data provider 1. The method of sending this request 212 is not limited to the method of using a public telephone line 204 and may be determined according to the type of the data and the type of the contract with the user. For example, mail can be adopted too. Further, it is also possible for the data provider A to provide the service according to a contract concluded in advance between the data provider A and the user B without sending a request 212.

Based on the request 212 from the user B, the data transmitting apparatus 201 converts the data transmitted to the data receiving apparatus 203 of the user B to a predetermined format, then transmits it as the data 210 to the communications satellite 202.

The communications satellite 202 relies the data 210 received from the data transmitting apparatus 201 and transmits the data 211 toward the ground.

The data 211 transmitted from the communications satellite 202 may be received by not only the data receiving apparatus 203 owned by the user B, but by the data receiving apparatuses of all users in a condition to receive the data. The data receiving apparatus 203 receives all of the data from the communications satellite 202 and from that selects and extracts the data responding to the request 212 which it had sent out itself.

Next, an explanation will be made of the data transmitting apparatus 201 shown in Fig. 3 with reference to Fig. 4.

The request 212 from the user B transmitted to the data transmitting apparatus 201 is picked up by a data request reception unit 301 and sent to a data management unit 302 (data 310).

The data management unit 302 performs the check of whether or not the contract information of the user B and request 212 have meaning. When there is no prob-

lem, it sends a reading request 311 to a data storage unit 303. The data storage unit 303 sends for example digital data 312 in accordance with the data reading request 310 to a data preparation unit 304.

The data preparation unit 304 prepares the digital data 312 from the data storage unit 303 by, for example, conversion of the data format such as the formation of an IP (Internet protocol) packet, encoding, formation of frames of for MAC (media access control), transportation of the MPEG (Moving Picture Experts Group) 2, etc. The conversion of the data format will be explained later.

The digital data 312 from the data storage unit 303, after being prepared or subjected to the format conversion by the data preparation unit 304, is sent as the data 210 to the communications satellite 202.

Next, an explanation will be made of the data receiving apparatus 203 shown in Fig. 3 with reference to Fig. 5.

The data 211 sent via the communications satellite 202 can be received by all users capable of receiving the data and is not limited to the data receiving apparatus 203 of the user B. The data receiving apparatus 203 receives all data from the communications satellite 202 and selects and receives the data in accordance with the request 212 issued by itself among them.

Namely, the data receiving apparatus 203 receives a large number of bits of data 211 containing transmitted data in accordance with the request 212 at the data receiving unit 401. The data receiving apparatus 203 selects the data directed to itself, the data which should be received by itself, and the data which can be received by itself (this is according to contract too) from among them. This selection is carried out at the data selection unit 402 of the data receiving apparatus 203. Note that, the data receiving apparatus 203 possessed by the user B is determined in advance by the contract between the user B and the data provider A. Accordingly, the specific data directed to another user cannot be selected by using the data receiving apparatus 203 possessed by the user B.

In the data selection unit 402, the data 310 which can be received by the user B is all sent to a data decomposing unit 403. The data directed to the user B sent to the data decomposing unit 403 is decomposed or decoded and becomes the digital data 412 which is sent to a data execution unit 404.

By this, only the user B can receive the data directed to the user B requested by the user B. This completes the data service.

Note that there are cases where the reception of the requested data is instantaneously carried out and a case where it continues for a long period. Where it is data of a type that is continuously received over a long period, the reception of the data is subsequently repeated in the data receiving apparatus 203 of the user B. The situation of this varies according to the type of the data requested by the user B.

Next, a detailed explanation will be made of the conversion of the data format of the transmitted data in the data transmitting apparatus 201.

First, an explanation will be made of the basic processing of the data preparation unit 304 of the data transmitting apparatus 201 of the data provider A by referring to Fig. 6.

In the data storage unit 303 in the data transmitting apparatus 201, the digital data required by the user is saved in an unprocessed form. The data storage unit 303 notified by the data management unit 302 that a reading request 311 of the data has come from the user B simultaneously sends the requested digital data 312 and the destination information 313 of the user B to the IP packet preparation unit 501 in the data preparation unit 304. Here, the direction information 313 of the user B is the IP address necessary for the IP packet transmission. In the data transmitting apparatus according to the present embodiment, inherent IP addresses are assigned to all contracted users. The IP address possessed by the user B is not possessed by users other than the user B during the period when the user B secures this.

The digital data 312 and the IP address 313 directed to the user B sent from the data storage unit 303 are sent to the IP packet preparation unit 501. In the IP packet preparation unit 501, the IP packet 510 is prepared by using the digital data 312 sent from the data storage unit 303 and the IP address 313 for specifying the user B at that point of time. The size of this IP packet is defined by the TCP/IP (transmission control protocol/Internet protocol). When the digital data requested by the user B exceeds that size, this digital data is divided into a plurality of IP packets and transferred to the next encoding unit 502.

The format of the IP packet 510 used in the data transmission apparatus according to the present embodiment is shown in Fig. 8.

VER (version) 701 is comprised of 4 bits and shows the version number of the IP protocol. It is used for confirming the compatibility of the IP. For example, when the version of the IP protocol is 4, the value of the VER 701 becomes "4".

IHL (Internet header length) 702 is comprised of 4 bits and shows the size of the IP packet header in units of 4 octets (32 bits). This is used for finding the head of a data field.

TOS (type of service) 703 is comprised of 8 bits and shows the quality of service requested by the transmitted datagram.

TL (total length) 704 is comprised of 16 bits and shows the total length, including the IP packet header and IP packet data field, in units of octets (8 bits).

ID (identification) 705 is comprised of 16 bits and is the identification number for distinguishing between the datagrams from the higher level.

FL (flags) 706 is comprised of 3 bits and shows information relating to the division of a datagram (frag-

ments). When the data is divided, this shows whether a fragment is intermediate or final.

FO (fragment offset) 707 is comprised of 13 bits and shows the position of the fragments in the original data in units of 8 octets.

TTL (Time To Live) 708 is comprised of 8 bits and shows the time (unit: seconds) at which a datagram set at the time of transmission is allowed to be present on the network. This is decremented by "1" every time the datagram passes a router. When this value becomes "0", the router discards the datagram without relaying it. This is to prevent the occurrence of excessive traffic on the network when loops occur on the network (datagrams unable to reach their destinations due to errors in the communications routing information circling around the same route) due to abnormalities in the routing.

PROT (protocol type) 709 is comprised of 8 bits and shows the protocol type code (no.) for identifying a higher protocol of the IP. For example, in the case of TCP (transmission control protocol), it becomes "6".

HC (Header Checksum) 710 is comprised of 16 bits and shows the checksum for detecting errors in the header field.

Source IP address 711 is comprised of 32 bits and shows the IP address of the terminal of the source of the IP packet. In the case of the embodiment shown in Fig. 3, the IP address of the data transmitting apparatus 201 enters.

The destination IP address 712 is comprised of 32 bits and shows the IP address of the terminal of the destination of the IP packet. In the case of the embodiment shown in Fig. 3, the IP address of the data receiving apparatus 203 enters.

The option and padding 713 are used when filling information other than the above information in the IP packet header.

Further, the digital data 312 from the data storage unit 303 in Fig. 3 enters in the data unit 713 in Fig. 8.

A detailed explanation of the IP protocol and packet header is given in Posutel, J. "Internet Protocol", STD 5, RFC 791, USC/Information Sciences Institute, September 1981.

Returning to the explanation of Fig. 6, the IP packet 510 prepared by the IP packet preparation unit 501 is transferred to the encoding unit 502.

The encoding unit 502 finds that the destination is the user B by the destination IP address 712 in the IP packet 510 and performs the encoding processing.

However, the encoding is not encoding of all or the data addressed to the user B. Depending on the type of the data 312, encoding is sometimes not performed. When encoding is not performed, the IP packet 510 is transferred directly from the IP packet preparation unit 501 to the MAC frame preparation unit 503. The encoding unit 502 will be explained in detail later.

The packet data 511 consisting of the IP packet 510 as a whole encoded by the encoding unit 502 is transferred to the MAC frame preparation unit 503. The format of a MAC frame is shown in Fig. 9. In the MAC frame preparation unit 503, the MAC header 902 shown in Fig. 9 is added to the packet data 511 addressed to the user B encoded by the encoding unit 502.

The destination IP address 801 in the MAC header 602 is comprised of 32 bits and is an IP address of the data receiving apparatus 203. Here, the destination IP address 801 of the MAC header 602 and the destination IP address in the encoded IP packet 511 are the same. In this way, the MAC header 602 is attached since the data receiving apparatus 203 can only learn of the destination IP address from the MAC header 602 at the time of receiving the data. That is, with just the encoded packet 511, the data receiving apparatus 203 cannot view the destination address until decoding the encoded IP packet 511 as a whole, so cannot determine if the packet is addressed to itself. Accordingly, in order for the data receiving apparatus 203 to learn if the IP packet is addressed to itself before decoding the received IP packet, it is necessary for the destination IP address 801 to be set in the header of the MAC frame. This destination IP address 801 is directly transferred from the IP packet preparation unit 501 to the MAC frame preparation unit 503.

Further, the PBL (padding byte length) 802 in the MAC header 602 shown in Fig. 9 is the padding byte length, that is, the length of the invalid data filled in for adjusting the size at the time of encoding. This is required for the user receiving the encoded IP packet to find the correct data length.

The CP (control packet) 803 is a bit enabling a user to identify if the necessary digital data or the control data necessary for system operation is contained. Normally, the CP 803 of a MAC frame 512 to be fetched by the user at the time of a request shows that not control data, but digital data is contained.

EN (encryption) 804 is a control bit for showing if the IP packet has been encoded by the encoding unit 502. By using this bit information, the user decides whether to decode the received MAC frame 512.

In the MAC frame preparation unit 503 of Fig. 6, the above control bit is added to an encoded (sometimes not encoded) IP packet 510.

The MAC frame 512 prepared by the MAC frame preparation unit 503 of Fig. 6 is transferred to the CRC calculation unit 504. The CRC calculation unit 504 calculates the CRC (cyclic redundancy checking) of all bytes of the sent MAC frame 512. In the present embodiment, the CRC has 16 bits. By performing the calculation of the CRC in this way, the data receiving apparatus 203 can check if the received MAC frame is correctly transmitted from the communications satellite 202. The CRC 806 of 16 bits generated in the CRC calculation unit 504 is added to the end of the MAC frame 512 as shown in Fig. 7 and Fig. 9.

The MAC frame 513 added with the CRC 806 is transferred to the section preparation unit 505 and converted to the section defined by the MPEG2. As shown

in Fig. 7, the MAC frame 513 is added immediately after the section header (SecHd). The format of the section header 603 is shown in Fig. 10.

The format of the section header 603 shown in Fig. 10 is defined by the MPEG2 and has a table ID 901, a section syntax indicator 902, a private indicator 903, a reserved 904, and a private section length 905. Here, the data length of the MAC frame 513 is in the private section length 905. The section 514 prepared at the section preparation unit 505 shown in Fig. 6 is transferred to the transport packet preparation unit 506. In the transport packet preparation unit 506, the transferred section format data is divided into the transport packets 515 and transferred to the next data transfer unit 507.

The format of the packet header (TSHd) 604 of the transport packet 515 shown in Fig. 7 is shown in Fig. 11. The header format of the transport packet 515 is defined by the MPEG2.

The SYNC byte 1001 is a 8 bit synchronization signal for detecting the head of a transport packet.

The error indicator 1002 is comprised of 1 bit and shows the presence of bit errors in a packet.

The payload unit start indicator 1003 is comprised of 1 bit and shows that a new PES packet has started from a payload (actual packet data) of a transport packet.

The transport packet priority 1004 is comprised of 1 bit and shows the degree of importance of the packet.

The PID (packet identification) 1005 is information for identifying the stream of 13 bits and shows the attributes of the individual streams of the packet.

The scramble control 1006 is comprised of 2 bits and shows the presence and type of the scrambling of the payload of the packet.

The adaptation field control 1007 is comprised of 2 bits and shows the presence of an adaptation field and the presence of a payload in the packet.

The continuity counter 1008 is comprised of 4 bits and is information for detecting if part of the packet having the game PID 1005 has been discarded in the interim by the continuity of the 4 bit cyclic count information.

Further, the size of a transport packet 515 is defined as 188 bytes, so in general it is necessary to divide one section 514 into a plurality of transport packets 515.

Here, usually, one section does not always have a length of a whole multiple of 184 bytes (byte number obtained by subtracting 4 bytes of the header length from 188 bytes), therefore, when dividing one section 514 into a plurality of transport packets 515, as shown in Fig. 3, data filling referred to as stuffing is carried out to form a stuffing region 605. Namely, where one section 514 which is not a multiple of 184 bytes is divided into a plurality of transport packets 515, a stuffing region 605 in which all bits "1" are stuffed is formed in the remaining data area of the last transport packet 515.

The section 514 divided into a plurality of transport packets 515 in this way is transferred to the data transmitting unit 507, passes through a data processing unit such as a multiplexer, and then transmitted to the communications satellite 202 and broadcasted.

The broadcasted multimedia data for the user B is received by the data receiving apparatus 203 of the user B and subjected to the reverse processing shown in Fig. 6 by the data decomposing unit 403. The finally requested multimedia data is delivered into the hands of the user B3.

The specific processing carried out in the data decomposing unit 403 of the data receiving apparatus 203 of the user B shown in Fig. 5 is basically an inverse algorithm to the algorithm in the data preparation unit 304 of the data transmitting apparatus 210.

First, in the data receiving unit 401 shown in Fig. 5, the transport packets 515 shown in Fig. 7 received via the communications satellite 202 are combined to generate a section 514. Next, the data receiving unit 401 expands the section 515 to generate the MAC frame 513 and outputs this to the data selection unit 402. Then, in the data selection unit 402, based on the destination IP address 801 shown in Fig. 9 contained in the MAC header 602 of the MAC frame 513 shown in Fig. 7, it is decided if this destination IP address 801 and the IP address of the data receiving apparatus 203 coincide. When they coincide, the data selection unit 402 selects the data and outputs the encoded IP packet 511 shown in Fig. 7 contained in this data to the data decomposing unit 403 as the data 411 shown in Fig. 5.

In the data decomposing unit 403, the encoded IP packet 511 shown in Fig. 7 input as the data 411 is decoded by using the secret key known only with the data provider A in advance, then the data error checking etc. are carried out. Here, for example, when for example there is a data error, processing for restoring the data is carried out or the data having the error is discarded.

As explained above, by using the TCP/IP communication protocol and, at the same time, providing a CRC bit in the IP packet, even if digital data is transmitted from the data transmitting apparatus 201 to the data receiving apparatus 203 via the communications satellite 202, data transmission error is effectively prevented from occurring and digital data transfer of a high quality can be realized.

Further, by transmitting the IP packet by the MAC frame system, the data can be transmitted to only the specific users.

Further, the data to be transmitted is encoded and only the data receiving apparatus 5 has a secret key for decoding this. Therefore stealing of the data by another person can be effectively prevented.

The present invention is not limited to the above embodiments. For example, the data compression method of the MAC frame is not limited to the MPEG2. Another compression method can also be used.

Further, the Internet protocol is not limited to the TCP/IP protocol. It is also possible to use for example an OSI (open systems interconnection) system.

Further, in the present embodiment, a case of using a secret key was exemplified as the encoding method, but a similar effect can be obtained even if a public key is used.

First Embodiment of Encoding Unit

Next, a more detailed explanation will be given of the IP packet preparation unit 501 and encoding unit 502 shown in Fig. 6 with reference to the drawings.

Figure 12 is a view showing a more detailed configuration of the first embodiment of the IP packet preparation unit 501 and encoding unit 502 shown in Fig. 6.

The IP packet preparation unit 501 and the encoding unit 502, as illustrated in Fig. 4, are provided an IP datagram composing unit 1201 for adding an IP packet header to the digital data 312 to be transmitted so as to form an IP packet 510 and an encoder 1202 for encoding the IP packet 510 using the encoding key 1205 to generate the encoded packet 511. The MAC frame preparation unit 503 shown in Fig. 6 has transferred to it encoded data 511 encoded at the encoder 1202 and an IP packet 510 output from the IP datagram composing unit 1201 and not encoded.

The IP packet preparation unit 501 and the encoding unit 502 further are provided with a modulator/demodulator (modem) 1203 for transmitting the decoding key through a public telephone line 204 and a signal processing device 1204 for performing signal processing and control processing. The signal processing device 1204 is for example comprised using a computer. The signal processing device 1204 performs the overall processing and control over the IP datagram composing unit 1201, the encoder 1202, and the modulator/demodulator (modem) 1203.

The IP datagram composing unit 1201 adds an IP packet header to the digital data 312 to be transmitted to generate an IP packet 510. At this time, the signal processing device 1204 judges based on the destination address 712 in the IP header whether to encode the digital data 312. When encoding it, it uses the encoder 1202, comprised as hardware, to encode the digital data 312 using the encoding key (encoding session key) 1205 as a key and sends the encoded data 511 to the MAC frame preparation unit 503. Note that the encoding key 7 is generated by the signal processing device 1204 based on the destination address 712 in the IP packet header.

When not encoding the digital data, the IP packet 510 is sent uncoded from the IP datagram composing unit to the MAC frame preparation unit 503.

At this time, the signal processing device 1204 controls a switch circuit 1206 in accordance with whether encoding is required or not to change the output signal to the MAC frame preparation unit 503.

Figure 13 is a flowchart showing the flow of the main processing of the apparatus shown in Fig. 12. At step S1301, the IP datagram composing unit 1201 adds the IP header to the digital data 312 which should be transmitted to generate an IP packet.

At step S1302, the encoding unit 1202 decides whether or not the data is to be encoded by viewing the destination address 712 contained in the IP header. Where it is to be encoded, the processing routine proceeds to step S1303, at which the encoding unit 1202 performs the encoding processing with respect to the digital data 312 which should be transmitted by using the encoding key 1205. Thereafter, the processing routine proceeds to step S1304, at which the encoded IP packet 511 is transferred to the MAC frame preparation unit 503 shown in Fig. 6.

Where it is decided at step S1302 that it is not to be encoded, the processing routine proceeds to step S1304, at which the IP packet 510 which is not encoded is transferred to the MAC frame preparation unit 503 shown in Fig. 6.

In the first embodiment, the encoder 1205 encodes just the IP packet data of the IP packet 510.

The operation routine and control are performed by the signal processing device 1204.

Separate from the transmission of the data using the satellite transmission line (large capacity transmission line), the apparatus uses the public telephone line 204 (small capacity transmission line) to transmit the decoding key 1405 corresponding to the encoding key 1205 from the data transmitting apparatus 201 to the data receiving apparatus 203 between the signal processing device 1204 and the modulator/demodulator (modem) 1203 and between the signal processing device 1404 and the modulator/demodulator (modem) 1403 on the data receiving apparatus 203 side shown in Fig. 14. By this, if the decoding key 1405 corresponding to the encoding key 1205 is used, the decoding of the encoded data 511 becomes possible in the data receiving apparatus 203.

Next, a detailed explanation will be given of the data decomposing unit 403 of the data receiving apparatus 203.

As explained in Fig. 5, in the data receiving apparatus 203, the data receiving unit 401 receives the data 211 from the satellite transmission line. The data selection unit 402 compares the destination IP address 801 in the MAC header 602 with the IP address allocated to the data receiving apparatus 203 to detect if they coincide. If they coincide, it enables reception by the user B and sends the data to the data decomposing unit 403.

Figure 14 will be used to explain a first embodiment of the data decomposing unit 403.

The IP datagram decomposing unit 101 decomposes the IP header from the digital data 411 sent from the data selection unit 402 and judges whether to decode it or not based on the information of the EN (encryption) 804 in the MAC header. The IP datagram

decomposing unit 1401 sends the received data minus the IP header to later circuits, for example, in the case of encoded data, to the decoder 1402 and in the case of plain text data, to the data execution unit 404.

When it should be decoded, the decoder 1402 constituted as hardware uses the decoding key (decoding use session key) 1405 to decode the encoded data 1410 after the decomposing of the IP header into the original data 1412 corresponding to the data 510 which should be transmitted in the data transmitting apparatus 201.

When the data is plain text which does not have to be decoded, the IP datagram decomposing unit 1410 decomposes the IP header and then extracts the original data corresponding to the digital data 510 to be transmitted in the data transmitting apparatus 201 through the switch circuit 1406 as the plain text data 1410 without decoding the same by using the decoding key.

Figure 15 is a flowchart showing the flow of the operation processing in the apparatus shown in Fig. 14.

At step S1501, the IP datagram decomposing unit 1401 of the data receiving apparatus 203 extracts the IP header from the data sent from the data selection unit 403 to generate the plain text data 1410 or the encoded data 1411.

At step S1502, the signal processing device 1404 decides whether to decode the encoded data 1411 using the decoding key 1405 based on the information embedded in the EN 804 in the MAC header. When using the decoding key 1405 to decode the encoded data 1411, the processing proceeds to step S1503, where the signal processing device 1404 makes the decoder 1402 perform decoding using the decoding key 1405 and then takes out the data at step S1504.

When not decoding using the decoding key 1405 at step S1502, the processing proceeds to step S1504, where the signal processing device 1404 takes out the plain text data 1410.

As explained above, a large amount of data such as video and audio (AV) data or computer data is encoded and transmitted according to need via the large capacity transmission line 152 such as a satellite transmission line. The encoded AV data can be effectively decoded only in the data receiving apparatus 153 to which the decoding key 1405 has been sent in advance from the transmitting apparatus 151 via a small capacity transmission line 156 such as the public telephone line. Accordingly, data receiving apparatuses 154 and 155 not effectively given the decoding key 1405 shown in Fig. 2, even if receiving encoded data via the satellite transmission line, will receive data having no meaning, thus tapping (stealing) from the data receiving apparatuses 154 and 155 of third persons can be substantially prevented.

A decoding key 1405 corresponding to the encoding key 1205 is transmitted via a public telephone line or other wired small capacity transmission line 156 having a high security compared with a satellite transmission line, therefore even if a tapper monitors only the large capacity transmission line 152, he will not see the decoding key 1405. Accordingly, even if data receiving apparatus 154 and 155 of third persons receive data from the satellite transmission line, if that data has been encoded, it cannot be effectively decoded and in actuality the data is not tapped.

Particularly, since a public telephone line or other small capacity transmission line 156 is a cable line performing one-to-one transmission between the transmitting apparatus 151 and the receiving apparatus 153, receiving apparatuses 14 and 155 intended for tapping are not connected to it, thus tapping or leakage is hard to occur compared with a large capacity transmission line 152 such as a satellite transmission line.

Second Embodiment of Encoding Unit

A second embodiment of the data transmission apparatus of the present invention will be explained next.

Figure 16 is a schematic view of the configuration of a data transmission apparatus according to a second embodiment of the present invention.

In the data transmission apparatus illustrated in Fig. 16, two receiving apparatuses 158 and 157 are connected to one transmitting apparatus 151 via a large capacity transmission line (first transmission system) 152 such as a satellite transmission line and a small capacity transmission line (second transmission system) 156, for example, a public telephone line, respectively. The receiving apparatus 154 is a receiving apparatus which is not normally connected to the transmitting apparatus 151 in the same way as the case illustrated in Fig. 2.

The configurations of the large capacity transmission line 152 and the small capacity transmission line 156 are similar to the configurations illustrated in Fig. 3.

In the second embodiment, the decoding key (decoding use session key) and the destination address used in the transmission using the large capacity transmission line 152 are transmitted from the transmitting apparatus 151 to two receiving apparatuses 158 and 157 via the small capacity transmission line 156. The destination address for a broadcast allocated for transmission all at once to a plurality of receiving apparatuses is used as the destination address at this time. The broadcast use destination address uses an IP address different from the IP address allocated individually to each receiving apparatus.

The receiving apparatuses 153 and 157 receiving the destination address from the transmitting apparatus 151 through the small capacity transmission line 156 compare the IP addresses at the data selection unit 502. At that time, they compare the received broadcast use destination address and the destination address 801 in the MAC header 602 sent through the large

capacity transmission line 152. By this, the receiving apparatus 153 or 157 can identify if the transmission was directed to itself.

The encoding and decoding processings in the second embodiment were explained using Fig. 12 to Fig. 15, but are the same as those in the first embodiment.

According to the second embodiment, the encoded data is transmitted to a plurality of (in this embodiment, two) receiving apparatuses 153 and 157 by using the large capacity transmission line 152 and can be decoded in the receiving apparatuses.

As an example of such an operation, for example, there are a case where the same encoded data is transmitted from the head office of a certain enterprise to a plurality of branch offices, a case where the encoded data is transmitted to all branch offices one time without transmitting the same to each of the plurality of branch offices, etc. Namely, there is an advantage in that the number of times of transmission can be reduced. Further, even in a case where pay video data is encoded and transmitted to many pay broadcast members, if the destination addresses of the receiving apparatuses on the pay broadcast members side are made the same, by once transmitting the encoded pay video data to these plurality of receiving apparatuses, they can be decoded at the valid receiving apparatus side.

Third Embodiment of Encoding Unit

A third embodiment of the data transmission apparatus of the present invention will be explained next.

The configuration of the data transmission apparatus of the third embodiment is similar to the configurations of the data transmission apparatuses of the first embodiment and the second embodiment mentioned by referring to Fig. 2, Fig. 12, Fig. 14, and Fig. 16. Provided, however, in the first embodiment and the second embodiment, before transmitting the encoded data from the large capacity transmission line 152, the decoding key (decoding session key) was transmitted from the transmitting apparatus 151 to the receiving apparatus 153 via the small capacity transmission line 156, but in the third embodiment, the encoding key (encoding session key) is transmitted in advance from the transmitting apparatus 151 to the receiving apparatus 153 via the small capacity transmission line 156. This encoding key is generated based on the destination address of the receiving apparatus 153 used in the data transmission using the large capacity transmission line 152 in the receiving apparatus 153, that is, the IP address of the receiving apparatus 153. In the receiving apparatus 153, the decoding key corresponding to the encoding key is learned by the preparation of the encoding key.

When the transmitted data is encoded in the transmitting apparatus 151, the encoding processing is carried out by using this encoding key.

The transmission of encoded data and the decoding processing thereof are similar to those of the first embodiment and the second embodiment.

In this third embodiment, the encoding key can be designated by the receiving apparatus 153 to the transmitting apparatus 151.

Fourth Embodiment of Encoding Unit

A fourth embodiment of the data transmission apparatus of the present invention will be explained next.

Figure 17 is a view of the configuration of the fourth embodiment of the IP packet preparation unit and encoding unit shown in Fig. 6.

The transmitting apparatus 151 and the receiving apparatus 153 are connected via a large capacity transmission line 152 and a small capacity transmission line 156. The connection configuration is similar to the connection configuration illustrated in Fig. 9.

The transmitting apparatus 151 has a modulator/demodulator (modem) 1203 connected to the small capacity transmission line 156, signal processing device 1204, encoding unit (data encoding unit) 1202, and IP datagram composing unit 1201 and, in addition, a key encoding unit 1701 and a key converter 1702. The key encoding unit 1701 generates the work key 1705 encoded from the master key 1703 and the work key 1704. The encoded work key 1705 is received at the modulator/demodulator (modem) 1403 of the receiving apparatus 203 through the modulator/demodulator (modem) 1203.

The IP datagram composing unit 1201 adds the IP header 14 having the destination address of the receiving apparatus 203 ,which is the destination of transmission of the encoded transmitted data, and a flag indicating whether or not the encoding processing is to be carried out to the digital data 312 which should be transmitted so as to compose the IP datagram 510. The destination address of the IP header is input to the key converter 1702 and used for generating the encoding key (encoding session key) 1205 in the key converter 1702 together with the work key 1704. In this way, the encoding key 1205 is generated based on the destination address of the receiving apparatus 203 in addition to the work key 1704, therefore even if the encoded transmitted data is received at a receiver other than the proper receiving apparatus 203, it cannot be properly decoded. Details of this will be explained later.

The encoding key (session key) 1205 generated by the key converter 1702 is used for encoding the data 510 which should be transmitted in the encoding unit 1202. The data which is encoded at the encoding unit 1202 and transmitted to the large capacity transmission line 152 is the encoded data 511.

The encoded data 511 is obtained by adding the not encoded IP header to the data obtained by encoding the data 510 which should be transmitted and transmitted to the MAC frame preparation unit 503.

Figure 18 is a view of the configuration of a fourth

embodiment of the data decomposing unit shown in Fig. 5.

The apparatus has the modulator/demodulator (modem) 1403 connected to the small capacity transmission line 156, the signal processing device 1404, the IP datagram decomposing unit 1401, the decoder (data decoder) 1402, and, in addition, a key decoder 1801 and a key converter 1802.

The key decoder 1802 decodes the work key 1804 using the work key 1705 and the master key 1803 which are received through the modulator/demodulator (modem) 1403 and encoded.

The IP datagram decomposing unit 1401 decomposes the IP header from the encoded data 411, extracts the destination address (IP address) of the receiving apparatus 203, and supplies this to the key converter 1802.

The key converter 1802 generates the decoding key (decoding session key) 1405 from the destination address and the decoded work key 1804. In the present embodiment, the decoding key 1405 is reproduced by using also the destination address, therefore the proper decoding key cannot be generated in the receiving apparatus which does not have the proper address.

Note that the destination address in the present embodiment not only means the IP address of a single apparatus, but also can mean (designate) a group constituted by a plurality of receiving apparatuses as explained in the second embodiment. In this case, the above encoding processing and decoding processing mean the encoding processing and decoding processing with respect to a plurality of apparatuses.

The decoding key 1405 converted at the key converter 1802 is used for decoding the encoded data 411 received through the large capacity transmission line 152.

The master key 1703 in the transmitting apparatus 201 and the master key 1803 in the receiving apparatus 203 have substantially the same contents. The master key 1703 (1803) is shared by the transmitting apparatus 201 and the receiving apparatus 203 by mailing an object on which the master key 1703 is recorded etc.

The transmitting apparatus 201 generates the work key 1704 and transmits the encoded key 1704 to the small capacity transmission line 156 via the modulator/demodulator (modem) 1203 to transmit this to the receiving apparatus 203. Further, it inputs the work key 1704 to the key converter 1702 and converts this to the encoding key 1205, encodes the digital data 312 which should be transmitted in the encoding unit 1202 by using the converted encoding key (encoding session key) 1205 as the key, and transmits the same as the encoded data 510 to the receiving apparatus 203 via the large capacity transmission line 152.

In the receiving apparatus 203, the encoded work key 1705 received from the small capacity transmission line 156 is decoded at the key decoder 1801 using the master key 1803 to decode the work key 1804. This is converted to the decoding key 1405 by the key converter 1802. The encoded data 411 received from the large capacity transmission line 152 is decoded at the decoder 1402 by using the converted decoding key (decoding session key) 1405 as the key.

The encoding processing of the work key in the transmitting apparatus 201 of the data transmission apparatus of the fourth embodiment is carried out so as to obtain the work key in the receiving apparatus 203 by using inherent information such as a serial number of the receiving terminal possessed by the receiving apparatus 203 which has been already shared by the transmitting apparatus 201 and the receiving apparatus 203 as a key (master key).

In the fourth embodiment, the encoded work key 1705 is transmitted through a small capacity transmission line 156, therefore even if there is leakage of the work key, there is almost no possibility of generation of the decoding key 1405 so far as the master key 1703 is not known. Therefore the security of the key transmission is very high. Accordingly, it is difficult for a receiving apparatus 203 of a third person to correctly decode the encoded data 411 transmitted through the large capacity transmission line 152 and the safety against also the leakage of information becomes higher.

Further, in the fourth embodiment, the generation (conversion) of the encoding key 1205 and the decoding key 1405 is carried out by using also the IP address of the receiving apparatus 203 of the destination of transmission, therefore the proper encoding unit 6 can be generated (reproduced) only in the proper receiving apparatus 203 and even if the encoded data 411 is received, the encoded data 411 cannot be correctly decoded.

First Modification of Fourth Embodiment

An example of encoding the work key 1704 in the transmitting apparatus 201 and transmitting the same as the encoded work key 1705 to the receiving apparatus 203 was shown in Fig. 17 as a preferred embodiment, but in the fourth embodiment, the encoding key 1205 and the decoding key 1405 are converted by using the IP address (destination address) of the receiving apparatus 201 and thus the security has become higher. Therefore, it is also possible to directly pass the work key 1704 through the small capacity transmission line 156 and use the same for the conversion of the decoding key (decoding session key) 1405 in the key converter 1802.

Namely, the key encoding unit 1701 in the transmitting apparatus 201 and the key decoder 1801 in the receiving apparatus 203 illustrated in Fig. 17 can be deleted. In this case, it is not necessary to store the master key 1703 in the apparatuses of the master key 1803, so the procedure between the transmitting apparatus 201 and the receiving apparatus 203 becomes simpler.

Second Modification of Fourth Embodiment

Further, the fourth embodiment explained referring to Fig. 17 gave, as a preferred embodiment, a case of generating the encoding key 1205 by using the work key 1704 and the destination address in the key converter 1702 in the transmitting apparatus 201 and encoding the data 510 using the encoding key 1205 at the encoder 1202, but as a simple example of the fourth embodiment, in the key converter 1702, the encoding key 1205 can be generated by using only the work key 1704 without using the destination address. In this case, the configuration of the key converter 1702 becomes simpler.

Similarly, also in the key converter 1802 in the receiving apparatus 203, it is possible to generate the decoding key 1405 by using the same master key 1803 as the master key 1703 and decode the received encoded data by using that decoding key 1405. Also in this case, the configuration of the key converter 1802 becomes simpler.

Third Modification of Fourth Embodiment

Further, it is also possible to combine the first modification and the second modification of the above fourth embodiment. Namely, according to the first modification of the fourth embodiment, the key encoding unit 1701 in the transmitting apparatus 201 and the key decoder 1801 in the receiving apparatus 201 illustrated in Fig. 17 are deleted and, according to the second modification, the configurations of the key converter 1702 and the key converter 1802 are made simpler.

Fifth Embodiment of Encoding Unit

A fifth embodiment of the data transmission apparatus of the present invention will be explained next.

Fig. 19 and Fig. 20 are views of the configuration of the fifth embodiment of the IP packet preparation unit and encoding unit shown in Fig. 6.

In the fourth embodiment, the encoded key 1705 was transmitted from the transmitting apparatus 201 to the receiving apparatus 203 by using a small capacity transmission line 156, but in the fifth embodiment, the encoded work key is transmitted from the receiving apparatus 203 to the transmitting apparatus 201 through the small capacity transmission line 156, and in the transmitting apparatus 201, the work key 1704 is decoded from the encoded work key 1705, and the encoding key 1205 is converted from this work key 1704.

For this reason, the transmitting apparatus 201 is provided with a key decoder 1901 equivalent to the key decoder 1801 in place of the key encoding unit 1701 illustrated in Fig. 17, and the receiving apparatus 203 is provided with a key encoding unit 2001 equivalent to the key encoding unit 1701 instead of the key decoder 1801 shown in Fig. 18. The rest of the configuration and operation are similar to those of the fourth embodiment.

In the fifth embodiment, the encoding key can be designated from the receiving apparatus 203 to the transmitting apparatus 201. The security of the key and the security of the encoding data 411 in the fifth embodiment are equivalent to those of the fourth embodiment.

Modification of Fifth Embodiment

In Fig. 19 and Fig. 20, as a preferred embodiment, an example was explained of encoding the work key 1804 at the receiving apparatus 203 and transmitting the encoded work key 1705 to the transmitting apparatus 201 through the small capacity transmission line 156, but in the fifth embodiment, similar to the fourth embodiment, the encoding key 1205 and the decoding key 1405 have been converted by using the destination address of the receiving apparatus 203, thus the security is high, and therefore it is also possible to directly send the work key 1804 through the small capacity transmission line 156 and use it for the conversion of the encoding key 1205 in the key converter 1702 of the transmitting apparatus 201.

Namely, the key decoder 1901 in the transmitting apparatus 201 and the key encoding unit 2001 in the receiving apparatus 203 can be deleted. In this case, the master key 1703 and the master key 1803 are no longer necessary, so the procedure becomes simple.

Other than this, also for the fifth embodiment, various simple configurations mentioned as modifications of the fourth embodiment can be adopted.

Sixth Embodiment of Encoding Unit

A sixth embodiment of the data transmission apparatus of the present invention will be explained next.

In the fourth embodiment and the fifth embodiment, in the transmitting apparatus 201 and the receiving apparatus 203, preferably, provision is made of a key converter 1702 for converting the work key 1704 to the encoding key (encoding session key (1205 and a key converter 1802 for converting the work key 1804 to the decoding key (decoding session key) 1405, as explained as the modification of the fourth embodiment, from the work key 1704 and the destination address.

Contrary to this, in the sixth embodiment, by using the input of the key converter 1702 of the transmitting apparatus 201 as the destination address in the transmission using the work key 1704 and the large capacity transmission line 152, the encoding key (encoding use session key) 1205 is generated from these information. Similarly, the input of the key converter 1802 of the receiving apparatus 203 is used as the work key 1804 and the IP address of the receiving apparatus 203, and the decoding key (decoding session key) 1405 is generated from these information. The rest of the configuration and operation are similar to those of the fourth

embodiment.

Note that, also in the sixth embodiment, the destination address not only means the IP address of a single apparatus, but also can mean (designate) a group constituted by a plurality of receiving apparatuses. In this case, the above encoding processing and decoding processing mean the encoding processing and decoding processing with respect to a plurality of apparatuses.

In the sixth embodiment, it is difficult for a person who does not know the destination address to generate the session key, therefore there is an advantage that the safety of the transmission of key becomes higher.

Seventh Embodiment of Encoding Unit

A seventh embodiment of the data transmission apparatus of the present invention will be explained next.

Fig. 21 is a view of the configuration of the seventh embodiment of the IP packet preparation unit and encoding unit of the present invention.

Fig. 22 is a view of the configuration of the seventh embodiment of the data decomposing unit shown in Fig. 5.

The transmitting apparatus 201 has the encoding unit 1202 and the key encoding unit 2101. The receiving apparatus 203 has the decoder 1402 and the key decoder 2201. Note that, for simplifying the explanation, in Fig. 21, the explanation of the IP datagram composing unit 1201, the signal processing device 1204, and the modulator/demodulator 1203 shown in Fig. 12 and, in Fig. 22, the explanation of the IP datagram decomposing unit 1401, signal processing device 1404, and modulator/demodulator 1403 shown in Fig. 14 are omitted. Also in the present embodiment, however, the processing of whether or not the processing and encoding of the destination data defined in the IP header 14 are to be performed is carried out similar to the above embodiments.

In the fourth embodiment, the encoded work key 1705 is transmitted from the transmitting apparatus 201 to the receiving apparatus 203 by using the small capacity transmission line 156, and in the fifth embodiment, the encoded work key 1705 is transmitted from the receiving apparatus 203 to the transmitting apparatus 201 by using the small capacity transmission line 156.

Contrary to this, in the seventh embodiment, the encoded session key 2102 is transmitted from the transmitting apparatus 201 to the receiving apparatus 203 by using the small capacity transmission line 156.

Further, where the number of receiving apparatus is one, the encoded session key 2102 is transmitted from the receiving apparatus 203 to the transmitting apparatus 201 by using the small capacity transmission line 156.

This encoding key (session key) 1205 is generated based on the destination address in the encoded data transmission using the large capacity transmission line 152.

In the transmitting apparatus 201, the encoding key (encoding session key) is generated, which is encoded by using the key encoding unit 2101 by using the master key 1703 shared by the transmitting apparatus 201 and the receiving apparatus 203 as the key, and the encoded session key 2102 is sent to the receiving apparatus 203 by using the small capacity transmission line 156. In the transmitting apparatus 201, the data 312 which should be transmitted is encoded by using the encoding unit 1202 using the generated encoding key 1205 as the key and sent to the MAC frame preparation unit 503.

The receiving apparatus 203 decodes the encoded session key 2102 received from the small capacity transmission line 156 by using the master key 1803 as the key to obtain the decoding key (decoding session key) 1405. In the receiving apparatus 203, the encoded date 411 received from the large capacity transmission line 152 is decoded at the decoder 1402 by using the decoding key 1405 found as described above as the key.

In the seventh embodiment, compared with the fourth embodiment and the fifth embodiment, the encoded session key 2102 is directly transmitted from the transmitting apparatus 201 to the receiving apparatus 203, therefore there is an advantage in configuration that the key converter 1702 and the key converter 1802 in the transmitting apparatus 201 and the receiving apparatus 203 are not required.

Eighth Embodiment of Encoding Unit

An eighth embodiment of the data transmission apparatus of the present invention will be explained next.

Figure 23 is a view of the configuration of the eighth embodiment of the IP packet preparation unit and encoding unit shown in Fig. 6.

The transmitting apparatus 201 has the IP datagram composing unit 1201 and the encoding unit 2302. The receiving apparatus 203 has the decoder 2402 and the IP datagram decomposing unit 1401.

In the transmitting apparatus 201, the data 312 which should be transmitted is input to the IP datagram composing unit 1201 and added with the IP header so as to form the IP datagram 510. The encoding unit 2302 encodes not only the IP packet data of the IP packet, but also the IP packet header. The data including the encoded data of the IP packet header is transmitted to the MAC frame preparation unit 503.

Fig. 24 is a view of the configuration of an eighth embodiment of the data decomposing unit shown in Fig. 5.

The receiving apparatus 203 decodes the data 411 encoded including the IP packet header received from

the large capacity transmission line 152 at the decoder 2402. The IP datagram decomposing unit 1401 decomposes the decoded IP packet and removes the IP data packet to obtain the data 412.

Note that, in the present embodiment, any of the above first to seventh embodiments can be applied to the transfer of the encoding key or information for generating the encoding key between the transmitting apparatus 201 and the receiving apparatus 203 using the small capacity transmission line 156 or the transfer of the decoding key or information for generating the decoding key between the transmitting apparatus 201 and the receiving apparatus 203. Namely, the present embodiment shows an example where also the IP header is also to be encoded. Any of the above embodiments can be applied to the transmission method of the encoding key or decoding key using the small capacity transmission line 156.

In the eighth embodiment, in the transmitting apparatus 201 or the receiving apparatus 203, a decision of whether or not the data being transmitted is encoded or decoded can be omitted.

In the eighth embodiment, the IP address used by only the user B is contained in the header of the IP packet 510, therefore it may seam that the encoding by the secret key used by only the user B is not necessary, but it becomes necessary so as to prevent another person from stealing the data directed to the user B by using the IP address of the user B and disguising itself as the user B.

Other Embodiments

In all of the above embodiments, as explained using Fig. 6, the IP packet preparation unit 501 prepared the IP packet, then the MAC frame preparation unit 503 prepared the MAC frames, but as shown in the first to the seventh embodiments, when encoding just the IP packet data without encoding the IP packet header of the IP packets, it is possible to omit the MAC frame preparation unit 503.

As shown in Fig. 8, the destination IP address 712 is embedded in the IP packet header, so by checking the IP packet header received at the receiving apparatus 203 side, it is possible to judge if the data is directed to itself without decoding the data.

Further, the information of the CP 803 and EN 804 in the MAC header 602 may be embedded in the option 712 of the IP packet header.

All of the above embodiments were illustrated for the case using the Internet protocol (IP), but in the working of the present invention, the invention is not limited to the Internet protocol. Other transmission protocol, for example, protocol according to ATM (asynchronous transfer mode) etc. can be used.

Also, in the working of the present invention, the above various embodiments can be appropriately combined.

As explained above, by transmitting information for generating the key for the processing of encoding or decoding by using a small capacity transmission line different from the large capacity transmission line for transmitting the data, the security of the transmission of the key is enhanced and thus the safety becomes high with respect to the leakage of the encoded data transmitted via the large capacity transmission line.

Further, by adding the destination data as the control information, it becomes possible to effectively decode the encoded data only in the proper receiving apparatus.

Further, by embedding information on the presence of coding of the data in the control information of the transmitted data, it is possible to judge the need of encoding and decoding by just viewing the control information necessary for the transmission.

Further, by using the TCP/IP communications protocol and providing a CRC bit in the IP packet, even when transmitting digital data from a transmitting apparatus through a communications satellite to a receiving apparatus, it is possible to effectively suppress the generation of data transmission errors and achieve a high quality digital data transfer.

Further, by transmitting by the MAC frame format, it is possible to not only deliver data by the broadcast format (simultaneous broadcast), but also to transmit data by a wireless format to just one or more specified users.

EXPLANATION OF REFERENCES

101	transmitting apparatus (transmitter)
102	receiving apparatus (receiver)
103	tapping apparatus (tapper)
104	data transmission line
105	data to be transmitted
106	encoder provided in transmitting apparatus
107	encoding key used for encoding in encoder (encoding session key)
108	decoding key (decoding session key)
109	decoder for decoding encoded data received from data transmission line using decoding key
110	decoded data

Claims

1. A data transmission apparatus connected to a first transmission system and a second transmission system, the data transmission apparatus comprising

a key transmitting means for transmitting through the second transmission system decoding key information for decoding encoded data sent through the first transmission system,

generating means for adding first transmission control information to the data to be encoded

and transmitted so as to generate transmitted data,

encoding means for generating encoded data from the transmitted data based on encoding key information corresponding to the decoding key information, and

data transmitting means for transmitting to the first transmission system the encoded data generated by the encoding means.

2. A data transmission apparatus as set forth in claim 1, wherein the communication capacity per unit time of the first transmission system is larger than the communication capacity per unit time of the second transmission system.

3. A data transmission apparatus as set forth in claim 2, wherein the first transmission system includes a satellite transmission line.

4. A data transmission apparatus as set forth in claim 3, wherein the second transmission system includes a cable transmission line.

5. A data transmission apparatus as set forth in claim 1, wherein the key transmitting means transmits destination information of the transmitted data along with the decoding key information through the second transmission system.

6. A data transmission apparatus as set forth in claim 5, wherein the key transmitting means transmits the same decoding key information and destination information to a plurality of receiving apparatuses connected to the first transmission line and the second transmission line.

7. A data transmission apparatus as set forth in claim 1, wherein the encoding means generates encoded data from the transmitted data based on the encoding key information and the destination information of the transmitted data.

8. A data transmission apparatus as set forth in claim 1, further comprising a key encoding means for encoding the work key information to generate decoding key information.

9. A data transmission apparatus as set forth in claim 8, wherein the encoding means generates encoded data from the transmitted data based on the work key information and the destination information of the transmitted data.

10. A data transmission apparatus as set forth in claim 1, wherein the first transmission control information includes the destination information of the transmitted data.

11. A data transmission apparatus as set forth in claim 10, wherein the first transmission control information includes an address defined by an Internet protocol as the destination information.

12. A data transmission apparatus as set forth in claim 10, wherein the encoding means encodes the transmitted data including the first transmission control information.

13. A data transmission apparatus as set forth in claim 10, wherein the encoding means adds to the transmitted data second transmission control information including the same destination information as the destination information included in the first transmission control information to generate the encoded data.

14. A data transmission apparatus as set forth in claim 13, wherein the encoding means adds a CRC check bit to generate the encoded data.

15. A data transmission apparatus as set forth in claim 13, wherein the second transmission control information includes information indicating the presence of coding of the data to be transmitted.

16. A data transmission apparatus as set forth in claim 15, wherein the second transmission control information includes information for distinguishing whether the data to be transmitted is information responding to a request from a receiving apparatus or whether it is control information for operating the communications system including the data transmitting apparatus.

17. A data transmitting apparatus connected to a first transmission system and a second transmission system, the data transmitting apparatus comprising

a key receiving means for receiving from the second transmission system encoding key information for encoding encoded data transmitted through the first transmission system,

a data generating means for adding control information to the data to be encoded and transmitted to generate transmitted data,

an encoding means for generating encoded data from the transmitted data based on the encoding key information, and

a data transmitting means for transmitting through the first transmission system the encoded data generated by the encoding means,

18. A data transmitting apparatus as sat forth in claim 17, wherein the encoding means comprises key decoding means for decoding the encoding key

information to generate work key information, and uses the work key information decoded by the key decoding means to generate encoded data.

19. A data transmitting apparatus as set forth in claim 18, wherein the encoding means generates encoded data based on the work key information and the destination information of the encoded data.

20. A data transmission method for transmitting data using a first transmission system and a second transmission system, the data transmission method comprising

a key transmitting step for transmitting through the second transmission system decoding key information for decoding encoded data transmitted through the first transmission system,
a data generating step for adding first transmission control information to the data to be encoded and transmitted to generate transmitted data,
an encoding step for generating encoded data from the generate transmitted data based on encoding key information corresponding to the decoding key information, and
a data transmitting step for transmitting the encoded data generated by the encoding step through the first transmission system.

21. A data transmission method as set forth in claim 20, wherein the communication capacity per unit time of the first transmission system is larger than the communication capacity per unit time of the second transmission system.

22. A data transmission method as set forth in claim 21, wherein the first transmission system includes a satellite transmission line.

23. A data transmission method as set forth in claim 21, wherein the second transmission system includes a cable transmission line.

24. A data transmission method as set forth in claim 20, wherein the key transmitting step transmits destination information of the transmitted data along with the decoding key information through the second transmission system.

25. A data transmission method as set forth in claim 24, wherein the key transmitting step transmits the same decoding key information and destination information to a plurality of receiving apparatuses connected to the first transmission line and the second transmission line.

26. A data transmission method as set forth in claim 20, wherein the encoding step generates encoded data from the transmitted data based on the encoding key information and the destination information of the transmitted data.

27. A data transmission method as set forth in claim 20, wherein further comprising a key encoding step for encoding the work key information to generate decoding key information.

28. A data transmission method as set forth in claim 27, wherein the encoding step generates encoded data from the transmitted data based on the work key information and the destination information of the transmitted data.

29. A data transmission method as set forth in claim 20, wherein the first transmission control information includes the destination information of the transmitted data.

30. A data transmission method as set forth in claim 29, wherein the first transmission control information includes an address defined by an Internet protocol as the destination information.

31. A data transmission method as set forth in claim 29, wherein the encoding step encodes the transmitted data including the first transmission control information.

32. A data transmission method as set forth in claim 29, wherein the encoding step adds to the transmitted data second transmission control information including the same destination information as the destination information included in the first transmission control information to generate the encoded data.

33. A data transmission method as set forth in claim 32, wherein the encoding step adds a CRC check bit to generate the encoded data.

34. A data transmission method as set forth in claim 32, wherein the second transmission control information includes information indicating the presence of coding of the data to be transmitted.

35. A data transmission method as set forth in claim 34, wherein the second transmission control information includes information for distinguishing whether the data to be transmitted is information responding to a request from a receiving apparatus or whether it is control information for operating the communications system including the data transmitting apparatus.

36. A data transmission method in a transmitting apparatus connected to a first transmission system and a second transmission system, the data transmission method comprising

a key receiving step for receiving from the second transmission system encoding key information for encoding encoded data transmitted through the first transmission system,
a data generating step for adding control information to the data to be encoded and transmitted to generate transmitted data,
an encoding step for generating encoded data from the transmitted data based on the encoding key information, and
a data transmitting step for transmitting through the first transmission system the encoded data generated by the encoding step.

37. A data transmission method as set forth in claim 36, wherein the encoding step includes a key decoding step for decoding the encoding key information to generate work key information, and uses the work key information decoded by the key decoding step to generate encoded data.

38. A data transmission method as set forth in claim 37, wherein the encoding step generates encoded data based on the work key information and the destination information of the encoded data.

39. A data receiving apparatus connected to a first transmission system over which encoded data is transmitted and a second transmission system over which key information is transmitted, the data receiving apparatus comprising

a key receiving means for receiving from the second transmission system decoding key information for decoding encoded data received from the first transmission system,
a data receiving means for receiving the decoded data from the first transmission system,
a data restoring means for deleting first transmission control information from the encoded data, and
a decoding means for decoding the encoded data from which the first transmission control information was deleted based on the decoding key information to generate decoded data.

40. A data receiving apparatus as set forth in claim 39, wherein the communication capacity per unit time of the first transmission system is larger than the communication capacity per unit time of the second transmission system.

41. A data receiving apparatus as set forth in claim 40, wherein the first transmission system includes a satellite transmission line.

42. A data receiving apparatus as set forth in claim 40, wherein the second transmission system includes a cable transmission line.

43. A data receiving apparatus as set forth in claim 39, wherein the key receiving means receives destination information of the encoded data along with the decoding key information from the second transmission system.

44. A data receiving apparatus as set forth in claim 43, wherein a plurality of receiving apparatuses are connected to the first transmission system, and the key receiving means receives the same decoding key information and destination information as other receiving apparatuses connected to the first transmission line and the second transmission line.

45. A data receiving apparatus as set forth in claim 39, wherein the decoding means generates decoded data from the received data based on the decoding key information and the destination information of the encoded data.

46. A data receiving apparatus as set forth in claim 39, wherein the decoding means includes key decoding means for decoding the decoding key information to generate work key information, and uses the work key information generated by the key decoding means to decode the encoded data.

47. A data receiving apparatus as set forth in claim 46, wherein the decoding means decodes the encoded data based on the work key information and the destination information of the encoded data.

48. A data receiving apparatus as set forth in claim 39, wherein the first transmission control information includes the destination information of the encoded data.

49. A data receiving apparatus as set forth in claim 48, wherein the first transmission control information includes an address defined by an Internet protocol as the destination information.

50. A data receiving apparatus as set forth in claim 48, wherein the decoding means decodes the encoded data which was encoded including the first transmission control information.

51. A data receiving apparatus as set forth in claim 48, wherein further provision is made of a judgement means for judging if the encoded data is directed to

itself based on the second transmission control information including the same destination information as the destination information included in the first transmission control information of the encoded data.

52. A data receiving apparatus as set forth in claim 51, wherein the judgement means judges if the encoded data is directed to itself and checks to the CRC check bit added to the encoded data to check for errors.

53. A data receiving apparatus as set forth in claim 51, wherein the judgement means judges if the encoded data is directed to itself end decides whether to decode or not based on the information indicating the presence of encoding included in the second transmission control information.

54. A data receiving apparatus as set forth in claim 53, wherein the second transmission control information includes information for distinguishing whether the received data is information responding to a request from its own receiving apparatus or whether it is control information for operating the communications system including the receiving apparatus.

55. A data receiving apparatus connected to a first transmission system and a second transmission system, the data receiving apparatus comprising

a key transmitting means for transmitting through the second transmission system encoding key information for preparing encoded data received from the first transmission system,
a data receiving means for receiving the encoded data encoded based on the encoding key information from the first transmission system,
a data restoring means for deleting the first transmission control information from the encoded data, and
a decoding means for decoding the encoded data based on decoding key information corresponding to the encoding key information.

56. A data receiving apparatus as set forth in claim 55, further comprising a key encoding means for encoding work key information to generate encoding key information.

57. A data receiving apparatus an set forth in claim 56, wherein the decoding means comprises a decoding key generating means for generating a decoding key based on the work key information and the destination information of the encoded data, and decodes the encoded data based on the decoding key generated by the decoding key generating means.

58. A data receiving method in a receiving apparatus connected to a first transmission system and a second transmission system, the data receiving method comprising

a key receiving step for receiving from the second transmission system decoding key information for decoding encoded data received from the first transmission system,
a data receiving step for receiving the decoded data from the first transmission system,
a data restoring step for deleting first transmission control information from the encoded data, and
a decoding step for decoding the encoded data from which the first transmission control information was deleted based on the decoding key information to generate decoded data.

59. A data receiving method as set forth in claim 58, wherein the communication capacity per unit time of the first transmission system is larger than the communication capacity per unit time of the second transmission system.

60. A data receiving method as set forth in claim 59, wherein the first transmission system includes a satellite transmission line.

61. A data receiving method as set forth in claim 59, wherein the second transmission system includes a cable transmission line.

62. A data receiving method as set forth in claim 58, wherein the key receiving step receives the destination information of the encoded data along with the decoded data from the second transmission system.

63. A data receiving method as set forth in claim 62, wherein the key receiving step receives the same decoding key information and destination information as other receiving apparatuses connected to the first transmission system and the second transmission system.

64. A data receiving method as set forth in claim 58, wherein the decoding step generates decoded data from the encoded data based on the decoding key information and the destination information of the encoded data.

65. A data receiving method as set forth in claim 58, wherein the decoding step includes key decoding

step for decoding the decoding key information to generate work key information, and uses the work key information generated by the key decoding step to decode the encoded data.

66. A data receiving method as set forth in claim 65, wherein the decoding step decodes the encoded data based on the work key information and the destination information of the encoded data.

67. A data receiving method as set forth in claim 58, wherein the first transmission control information includes the destination information of the encoded data.

68. A data receiving method as set forth in claim 67, wherein the first transmission control information includes an address defined by an Internet protocol as the destination information.

69. A data receiving method as set forth in claim 67, wherein the decoding step decodes the encoded data which was encoded including the first transmission control information.

70. A data receiving method as set forth in claim 67, wherein further comprising a judgement step for judging if the encoded data is directed to itself based on the second transmission control information including the same destination information as the destination information included in the first transmission control information of the encoded data.

71. A data receiving method as set forth in claim 70, wherein the judgement step judges if the encoded data is directed to itself and checks to the CRC check bit added to the encoded data to check for errors.

72. A data receiving method as set forth in claim 70, wherein the judgement step judges if the encoded data is directed to itself and decides whether to decode or not based on the information indicating the presence of encoding included in the second transmission control information.

73. A data receiving method as set forth in claim 72, wherein the second transmission control information includes information for distinguishing whether the received data is information responding to a request from its own receiving apparatus or whether it is control information for operating the communications system including the receiving apparatus.

74. A data receiving method in a receiving apparatus connected to a first transmission system and a second transmission system, the data receiving method comprising

a key transmitting step for transmitting through the second transmission system encoding key information for preparing encoded data received from the first transmission system,
a data receiving step for receiving the encoded data encoded based on the encoding key information from the first transmission system,
a data restoring step for deleting the first transmission control information from the encoded data, and
a decoding step for decoding the encoded data based on decoding key information corresponding to the encoding key information.

75. A data receiving method as set forth in claim 74, wherein further provision is made of a key encoding step for encoding work key information to generate encoding key information.

76. A data receiving method as set forth in claim 75, wherein the decoding includes a decoding key generating step for generating decoding key information based on the work key information and the destination information of the encoded data, and decodes the encoded data based on the decoding key generated by the decoding key generating step.

77. A data transmission apparatus having a first transmission system and a second transmission system, the data transmission apparatus comprising:

a transmitting apparatus having

a key transmitting means for transmitting through the second transmission system decoding key information for decoding the encoded data transmitted through the first transmission system,
a data generating means for generating transmitted data added with first transmission control information from the data to be encoded and transmitted,
an encoding means for generating encoded data from the transmitted data based on encoding key information corresponding to the decoding key information, and
a data transmitting means for transmitting through the first transmission system the encoded data generated by the encoding means and

a receiving apparatus having

a key receiving means for receiving from

the second transmission system decoding key information for decoding the encoded data received from the first transmission system,

a data receiving means for receiving the encoded data from the first transmission system, data restoring means for deleting first transmission control information from the encoded data, and

a decoding means for decoding the encoded data based on the decoding key information.

78. A data transmission apparatus having a first transmission system and a second transmission system, the data transmission apparatus comprising:

a transmitting apparatus having

a key receiving means for receiving from the second transmission system encoding key information for encoding the encoded data transmitted through the first transmission system,

a data generating means for generating transmitted data added with control information from the data to be encoded and transmitted,

an encoding means for generating encoded data from the transmitted data based on encoding key information, and

a data transmitting means for transmitting through the first transmission system the encoded data generated by the encoding means and

a receiving apparatus having

a key transmitting means for transmitting through the second transmission system encoding key information for preparing the encoded data received from the first transmission system,

a data receiving means for receiving the encoded data encoded based on the encoding key information from the first transmission system,

a data restoring means for deleting first transmission control information from the encoded data, and

a decoding means for decoding the encoded data based on decoding key information corresponding to the encoding key information.

79. A data transmission method using a transmission apparatus having a first transmission system and a second transmission system, the data transmission method comprising:

a transmitting processing step having

a key transmitting step for transmitting through the second transmission system decoding key information for decoding the encoded data transmitted through the first transmission system,

a data generating step for generating transmitted data added with first transmission control information from the data to be encoded and transmitted,

an encoding step for generating encoded data from the transmitted data based on encoding key information corresponding to the decoding key information, and

a data transmitting step for transmitting through the first transmission system the encoded data generated by the encoding step and

a receiving processing step having

a key receiving step for receiving from the second transmission system decoding key information for decoding the encoded data received from the first transmission system,

a data receiving step for receiving the encoded data from the first transmission system,

a data restoring step for deleting first transmission control information from the encoded data, and

a decoding step for decoding the encoded data based on the decoding key information.

80. A data transmission method for transmission of data using a transmission apparatus having a first transmission system and a second transmission system, the data transmission method comprising:

a transmitting processing step having

a key receiving step for receiving from the second transmission system encoding key information for encoding the encoded data transmitted through the first transmission system,

a data generating step for generating transmitted data added with control information from the data to be encoded and transmitted,

an encoding step for generating encoded data from the transmitted data based on encoding key information, and

a data transmitting step for transmitting through the first transmission system the encoded data generated by the encoding step and

a receiving processing step having

a key transmitting step for transmitting through the second transmission system encoding key information for preparing the encoded data received from the first transmission system,
a data receiving step for receiving the encoded data encoded based on the encoding key information from the first transmission system,
a data restoring step for deleting first transmission control information from the encoded data, and
a decoding step for decoding the encoded data based on decoding key information corresponding to the encoding key information.

FIG. 1

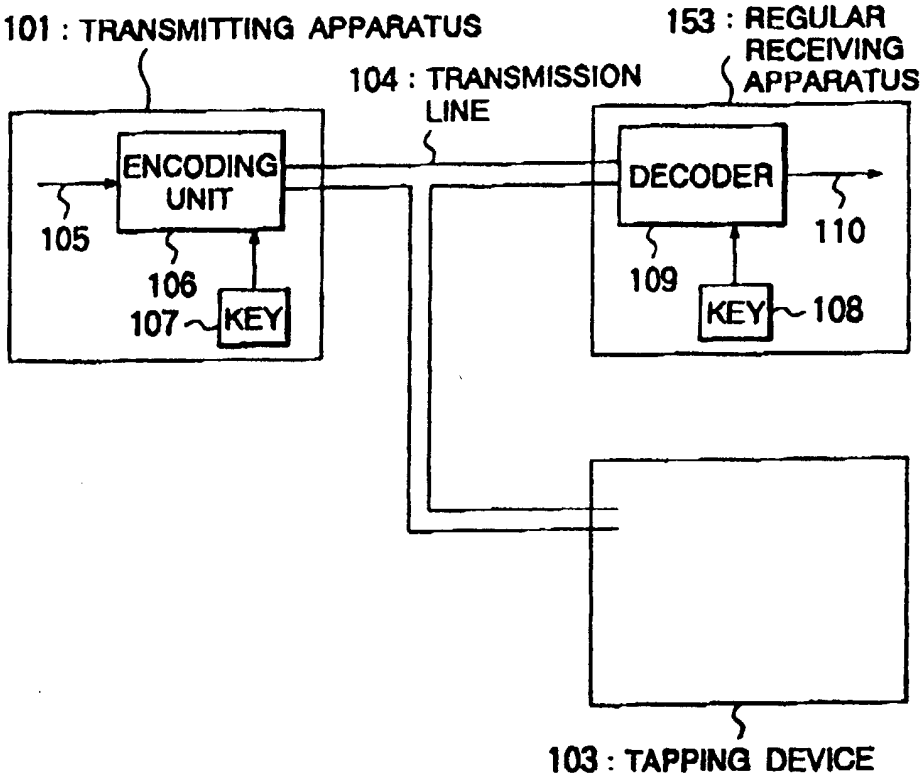

101 : TRANSMITTING APPARATUS
153 : REGULAR RECEIVING APPARATUS
104 : TRANSMISSION LINE
ENCODING UNIT
105
106
107
KEY
DECODER
110
109
KEY
108
103 : TAPPING DEVICE

FIG. 2

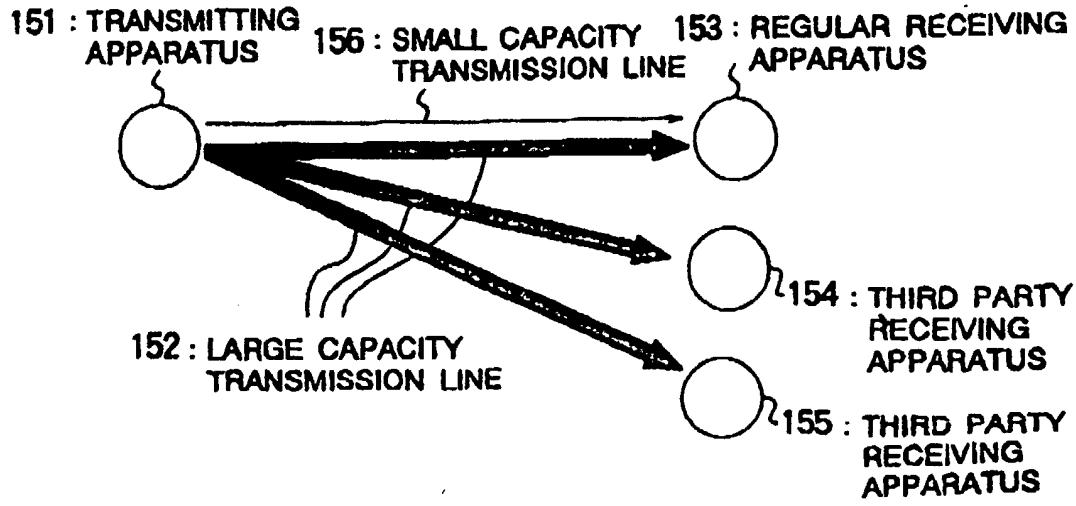

151 : TRANSMITTING APPARATUS
156 : SMALL CAPACITY TRANSMISSION LINE
153 : REGULAR RECEIVING APPARATUS
154 : THIRD PARTY RECEIVING APPARATUS
152 : LARGE CAPACITY TRANSMISSION LINE
155 : THIRD PARTY RECEIVING APPARATUS

FIG. 3

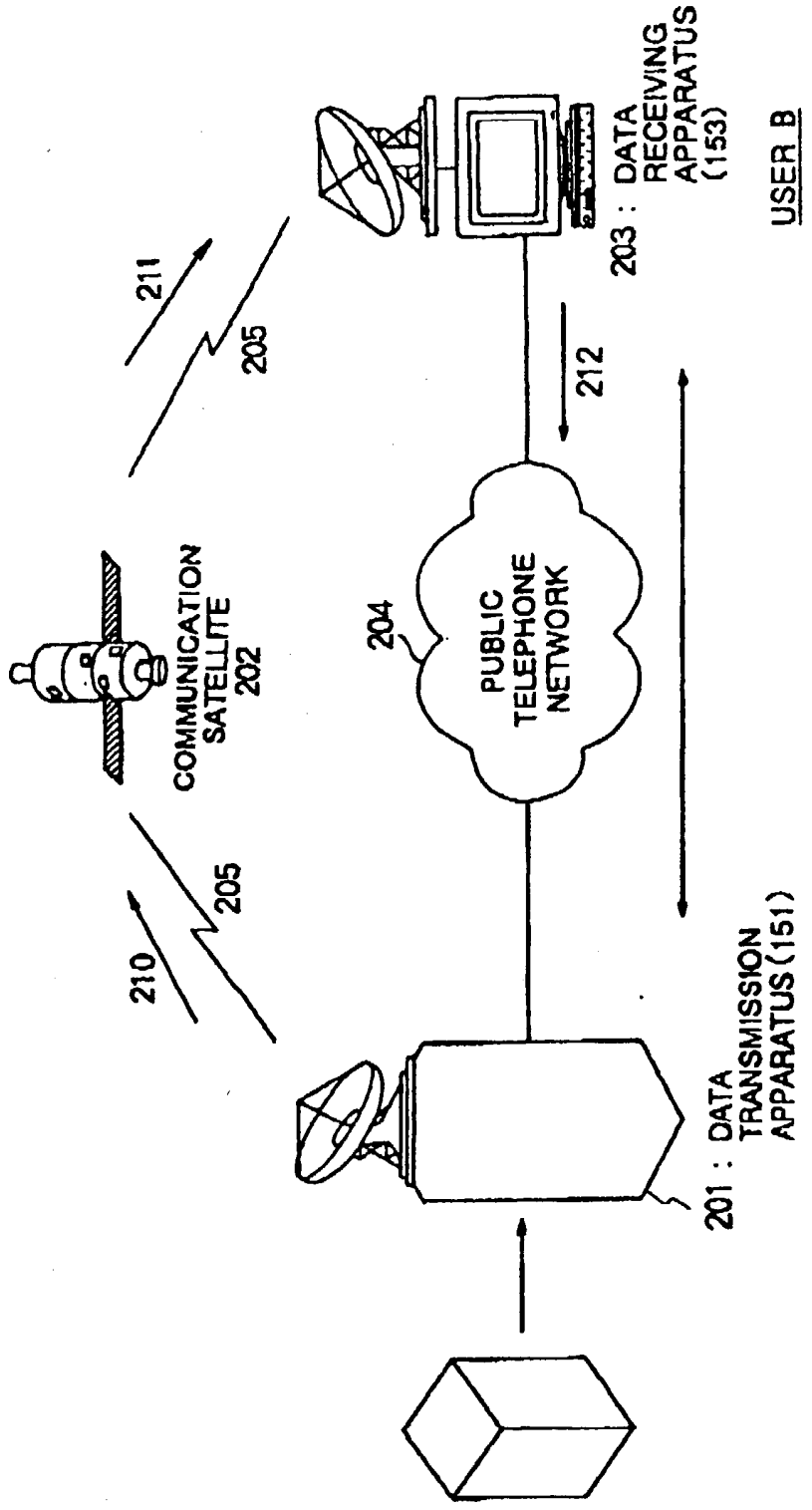

211
205
210
205
COMMUNICATION SATELLITE 202
204
PUBLIC TELEPHONE NETWORK
212
203 : DATA RECEIVING APPARATUS (153)
USER B
201 : DATA TRANSMISSION APPARATUS (151)
DATA PROVIDER A

FIG. 4

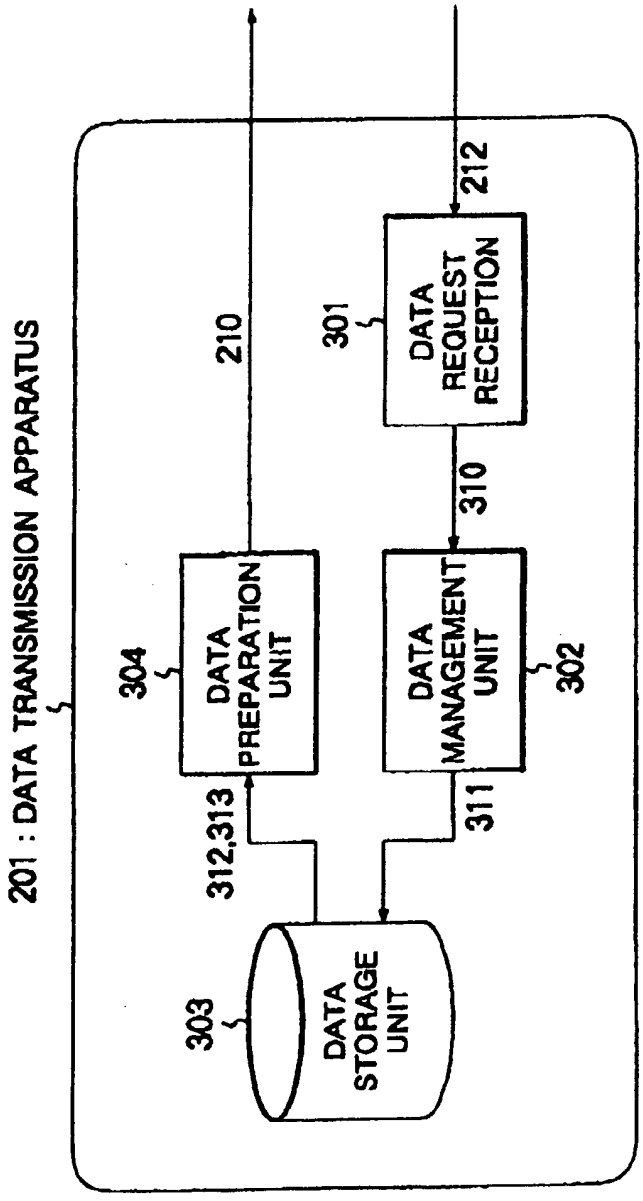

201 : DATA TRANSMISSION APPARATUS
210
212
301
DATA REQUEST RECEPTION
310
304
DATA PREPARATION UNIT
DATA MANAGEMENT UNIT
302
312,313
311
303
DATA STORAGE UNIT

FIG. 5

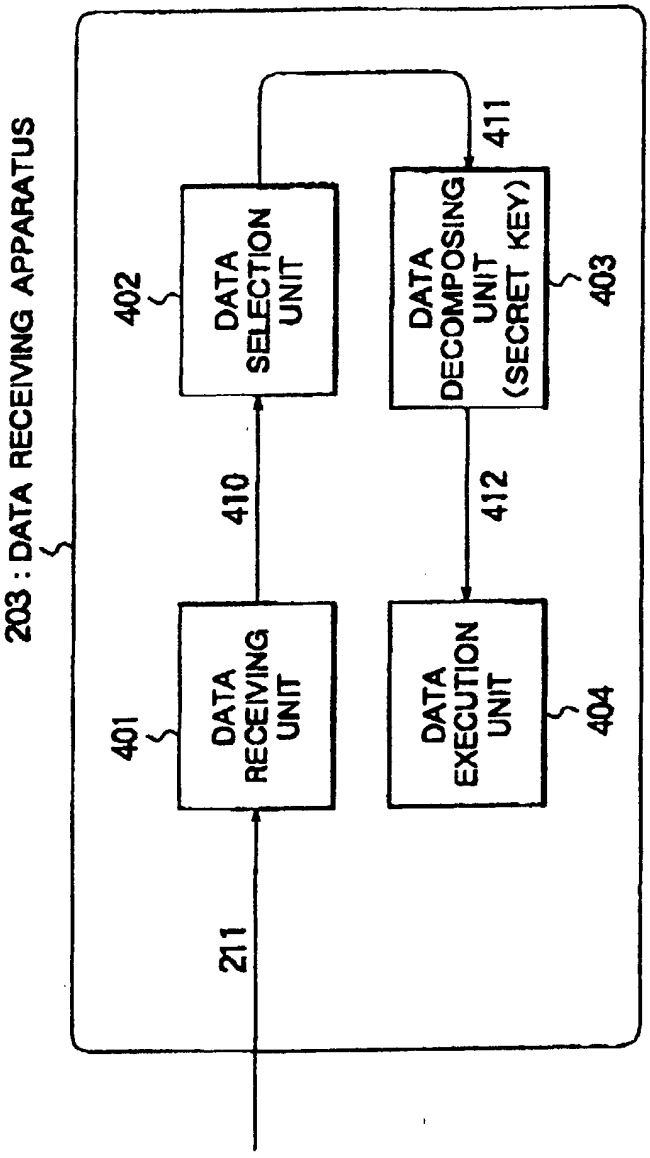

203 : DATA RECEIVING APPARATUS
401
DATA RECEIVING UNIT
402
DATA SELECTION UNIT
403
DATA DECOMPOSING UNIT (SECRET KEY)
404
DATA EXECUTION UNIT
410
411
412
211

FIG. 6

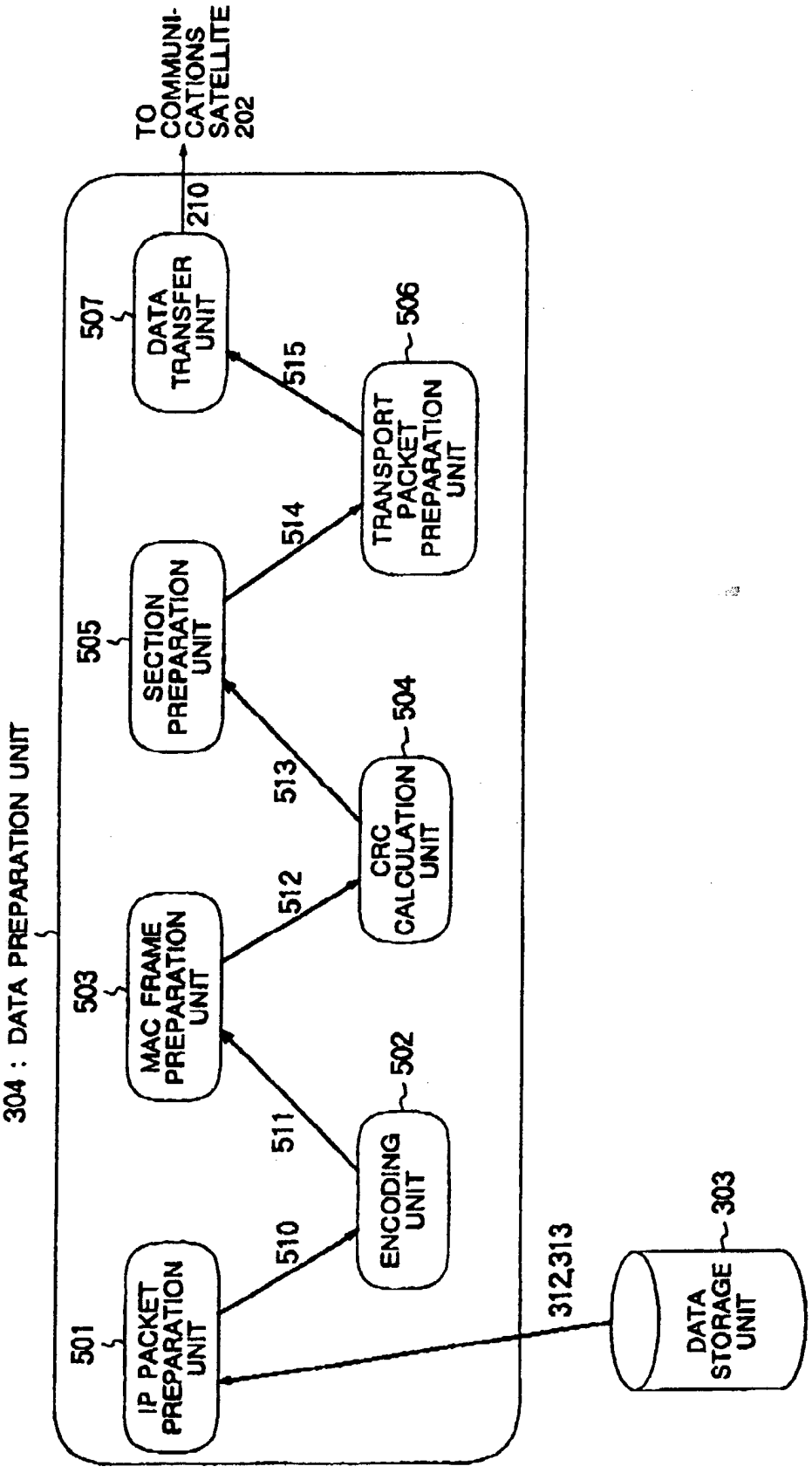

304 : DATA PREPARATION UNIT
501
IP PACKET PREPARATION UNIT
503
MAC FRAME PREPARATION UNIT
505
SECTION PREPARATION UNIT
507
DATA TRANSFER UNIT
502
ENCODING UNIT
504
CRC CALCULATION UNIT
506
TRANSPORT PACKET PREPARATION UNIT
510
511
512
513
514
515
210
TO COMMUNI-CATIONS SATELLITE 202
312,313
303
DATA STORAGE UNIT

FIG. 7

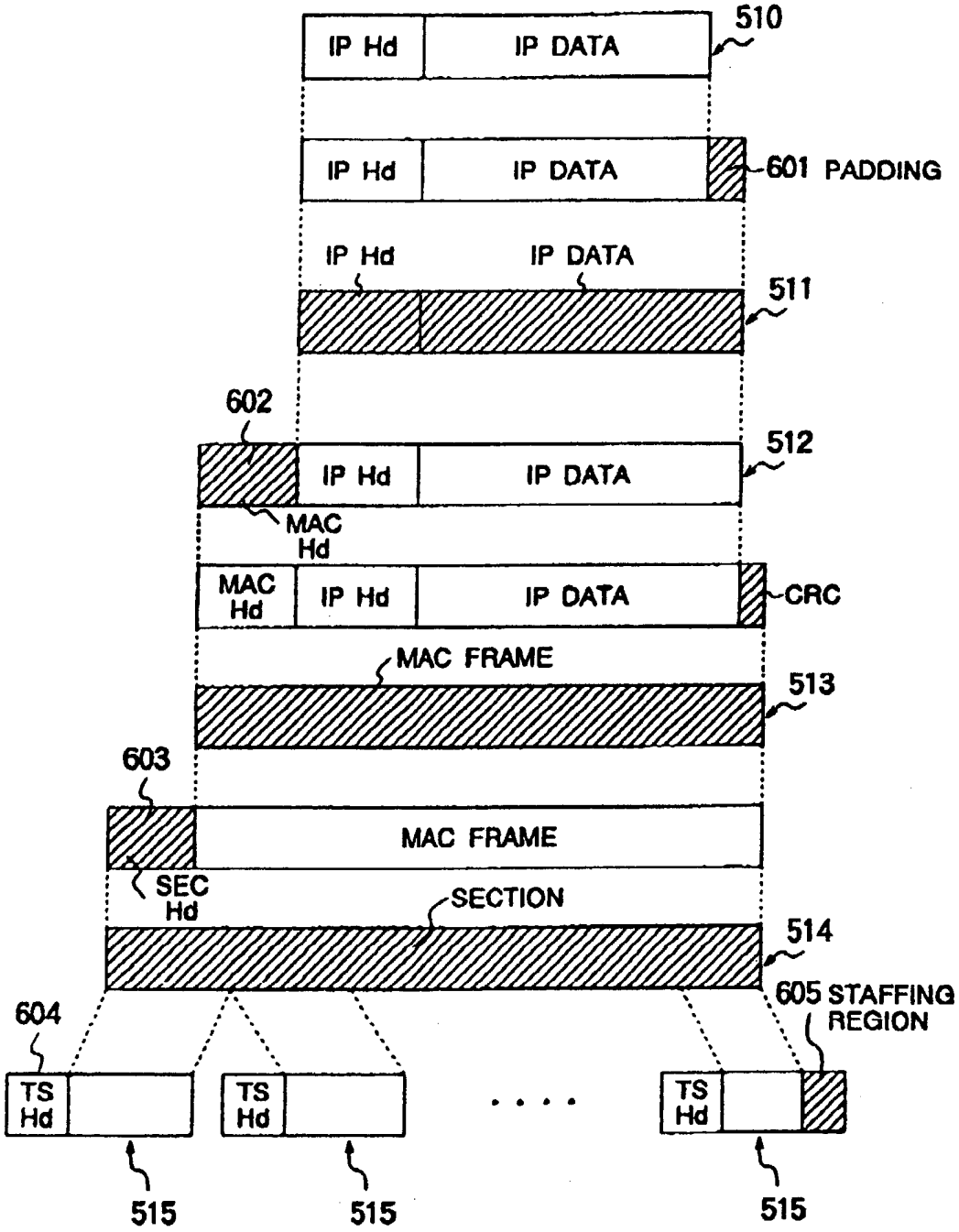

IP Hd
IP DATA
510
IP Hd
IP DATA
601 PADDING
IP Hd
IP DATA
511
602
IP Hd
IP DATA
512
MAC Hd
MAC Hd
IP Hd
IP DATA
CRC
MAC FRAME
513
603
MAC FRAME
SEC Hd
SECTION
514
605 STAFFING REGION
604
TS Hd
TS Hd
TS Hd
515
515
515

FIG. 8

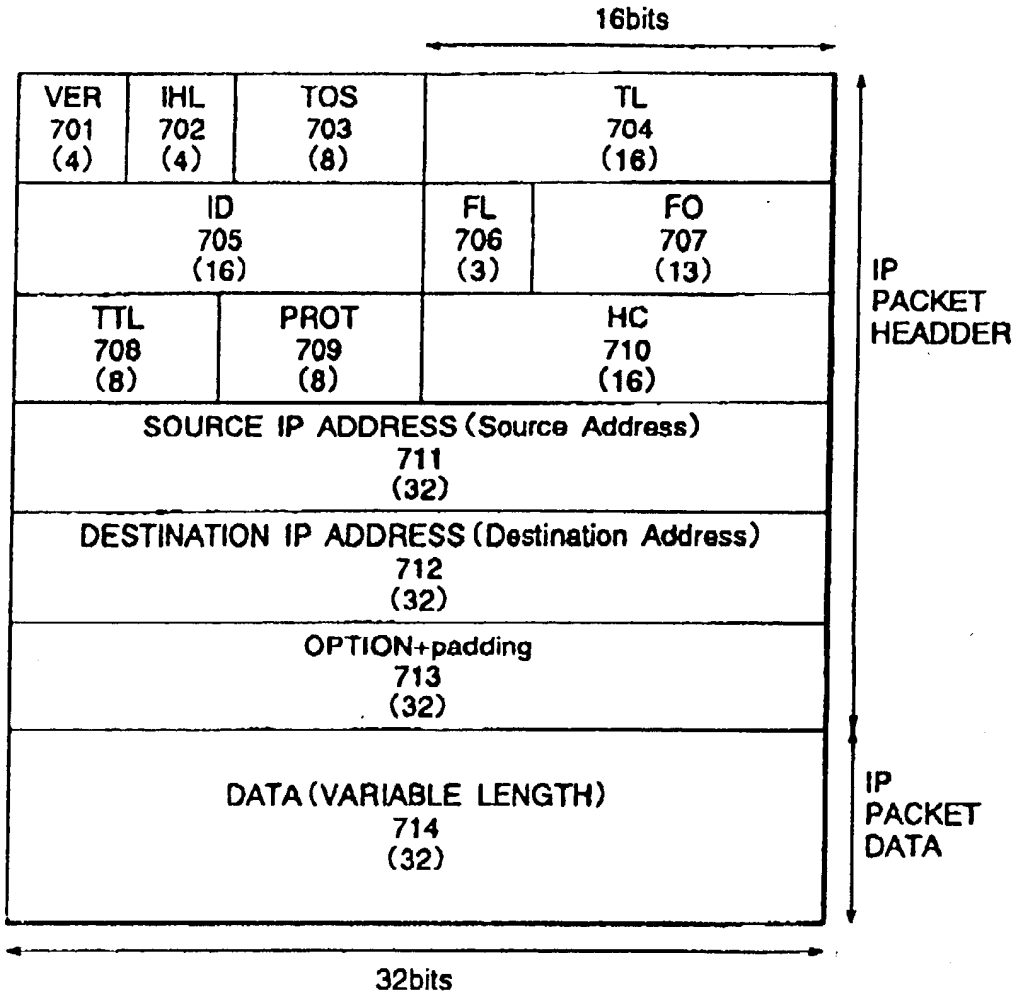

16bits
VER
701
(4)
IHL
702
(4)
TOS
703
(8)
TL
704
(16)
ID
705
(16)
FL
706
(3)
FO
707
(13)
TTL
708
(8)
PROT
709
(8)
HC
710
(16)
SOURCE IP ADDRESS (Source Address)
711
(32)
DESTINATION IP ADDRESS (Destination Address)
712
(32)
OPTION+padding
713
(32)
DATA (VARIABLE LENGTH)
714
(32)
IP PACKET HEADDER
IP PACKET DATA
32bits

FIG. 9

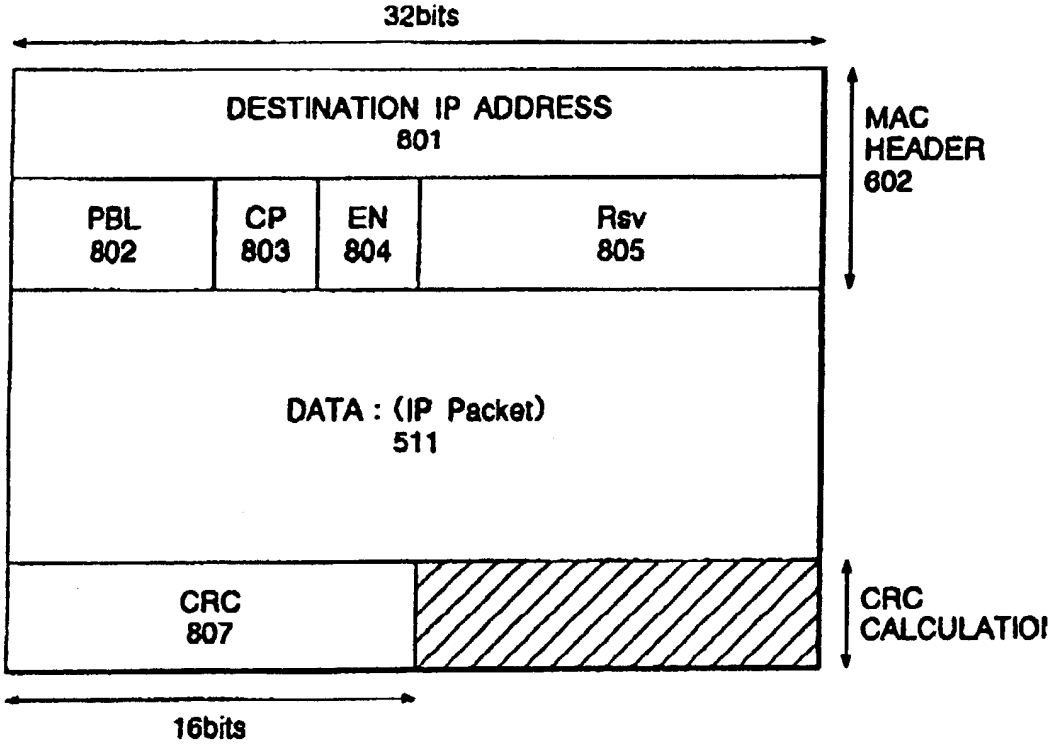
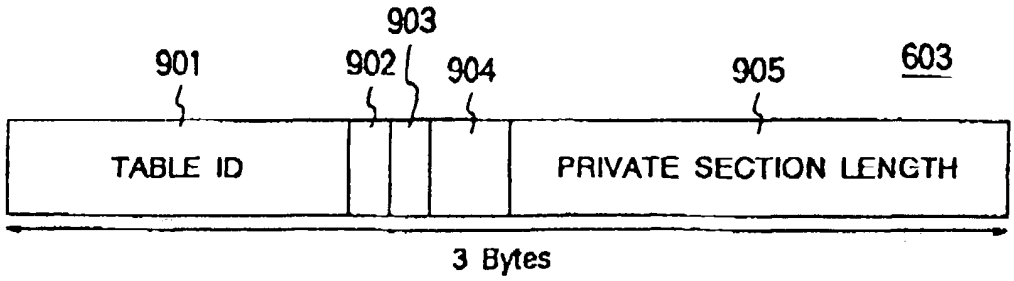
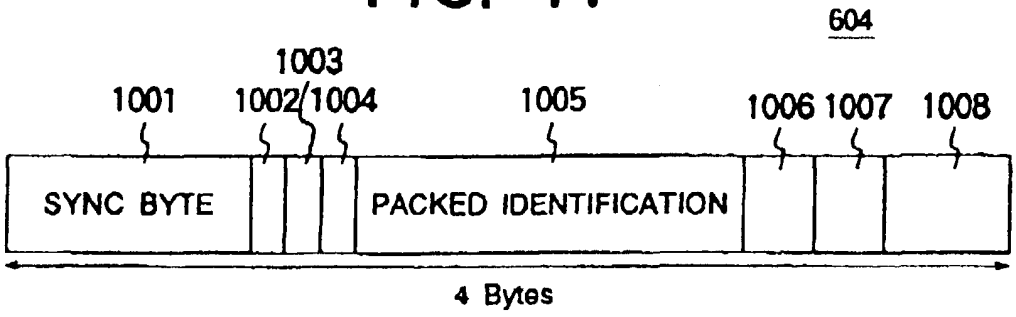

32bits
DESTINATION IP ADDRESS
801
PBL
802
CP
803
EN
804
Rsv
805
MAC
HEADER
602
DATA : (IP Packet)
511
CRC
807
CRC
CALCULATIO
16bits

FIG. 10



902 : SECTION SYNTAX INDICATOR
903 : PRIVATE INDICATOR
904 : RESERVED

FIG. 11



1002 : ERROR INDICATOR
1003 : PAYLOAD START INDICATOR
1004 : TRANSPORTPACKET PRIORITY
1006 : SCRAMBLE CONTROL
1007 : ADAPTATION FIELD CONTROL
1008 : CONTINUITY COUNTER

FIG. 12

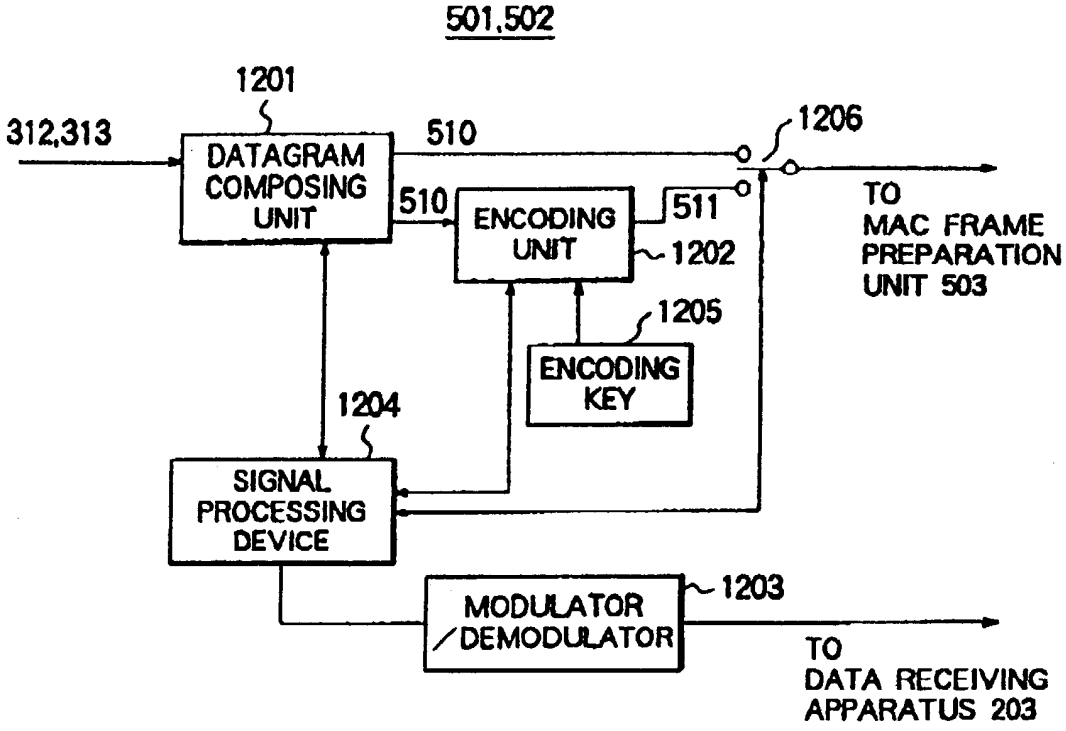

501,502
1201
312,313
DATAGRAM COMPOSING UNIT
510
1206
510
ENCODING UNIT
511
1202
TO MAC FRAME PREPARATION UNIT 503
1205
ENCODING KEY
1204
SIGNAL PROCESSING DEVICE
MODULATOR /DEMODULATOR
1203
TO DATA RECEIVING APPARATUS 203

FIG. 13

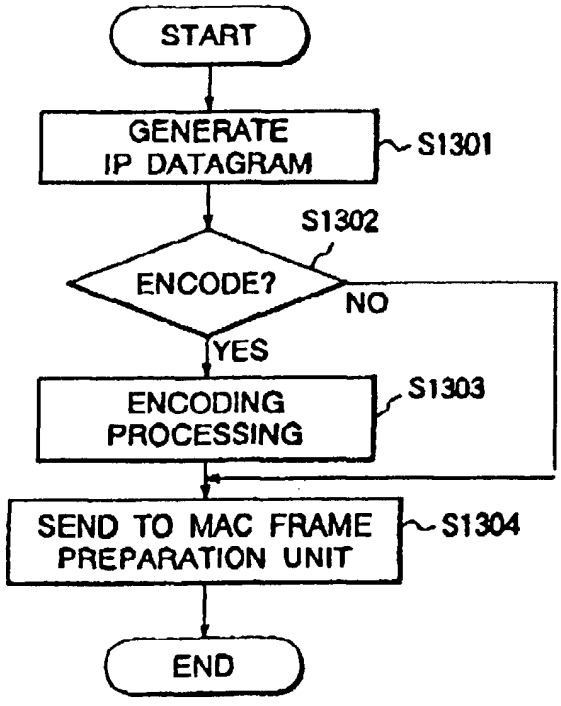

START
GENERATE IP DATAGRAM
S1301
S1302
ENCODE?
NO
YES
ENCODING PROCESSING
S1303
SEND TO MAC FRAME PREPARATION UNIT
S1304
END

FIG. 14

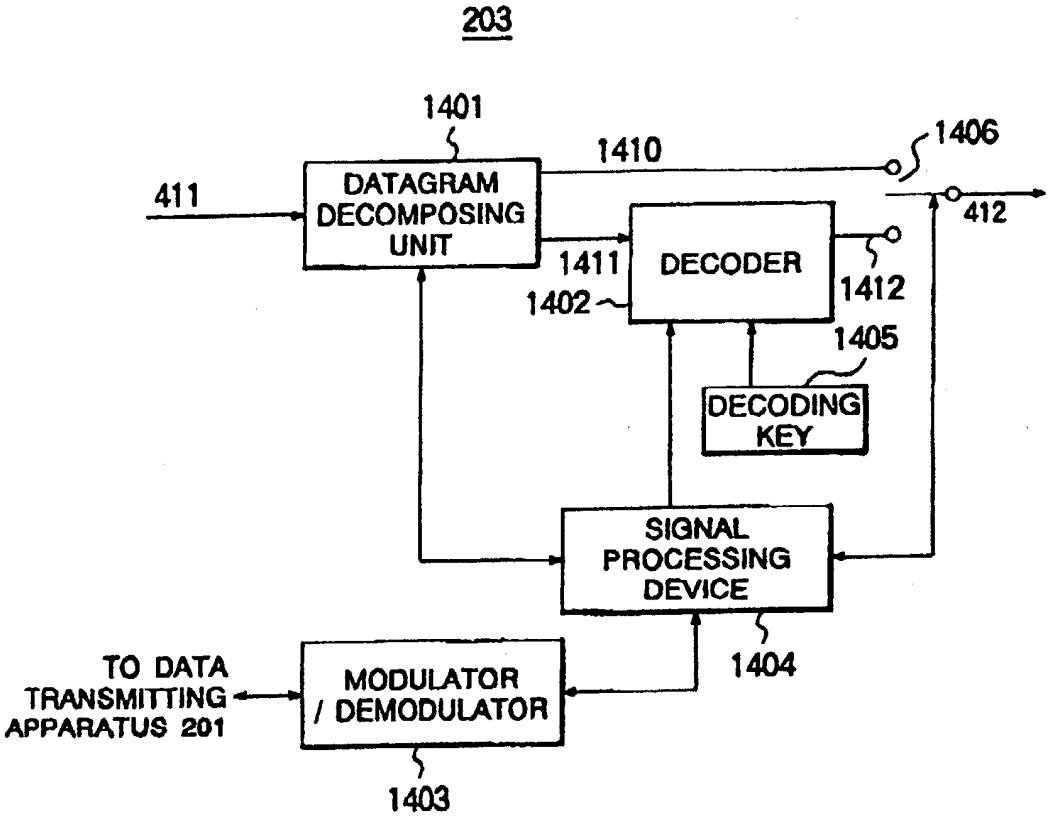

203
1401
1406
1410
411
DATAGRAM DECOMPOSING UNIT
412
1411
DECODER
1412
1402
1405
DECODING KEY
SIGNAL PROCESSING DEVICE
1404
TO DATA TRANSMITTING APPARATUS 201
MODULATOR / DEMODULATOR
1403

FIG. 15

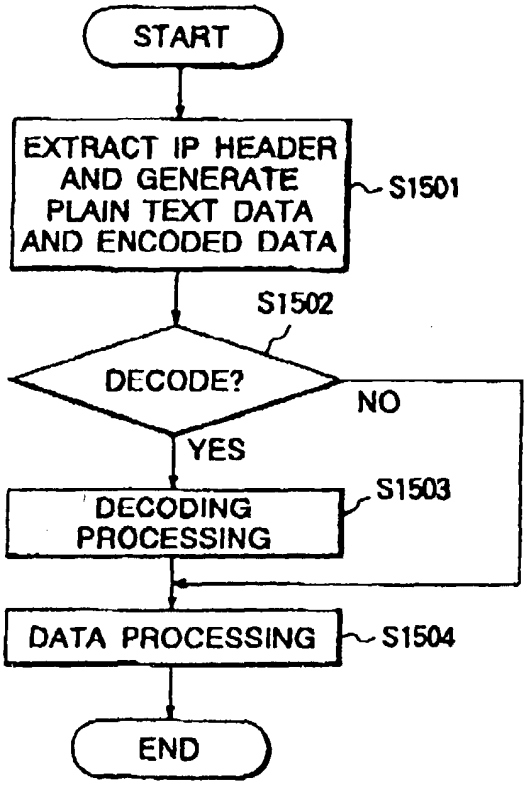

START
EXTRACT IP HEADER AND GENERATE PLAIN TEXT DATA AND ENCODED DATA
S1501
S1502
DECODE?
NO
YES
DECODING PROCESSING
S1503
DATA PROCESSING
S1504
END

FIG. 16

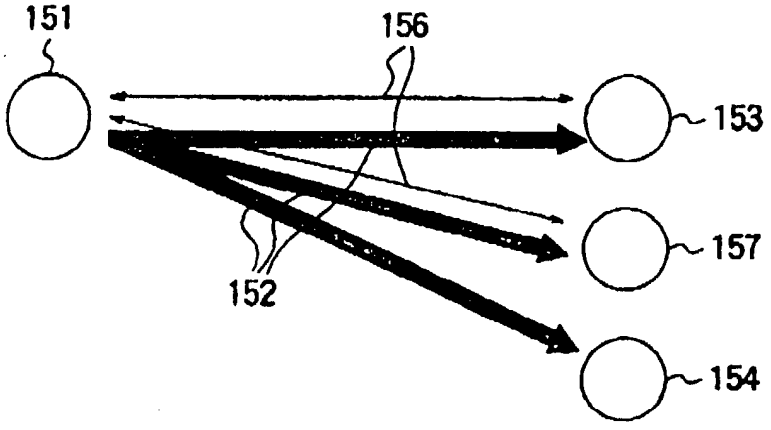


FIG. 17

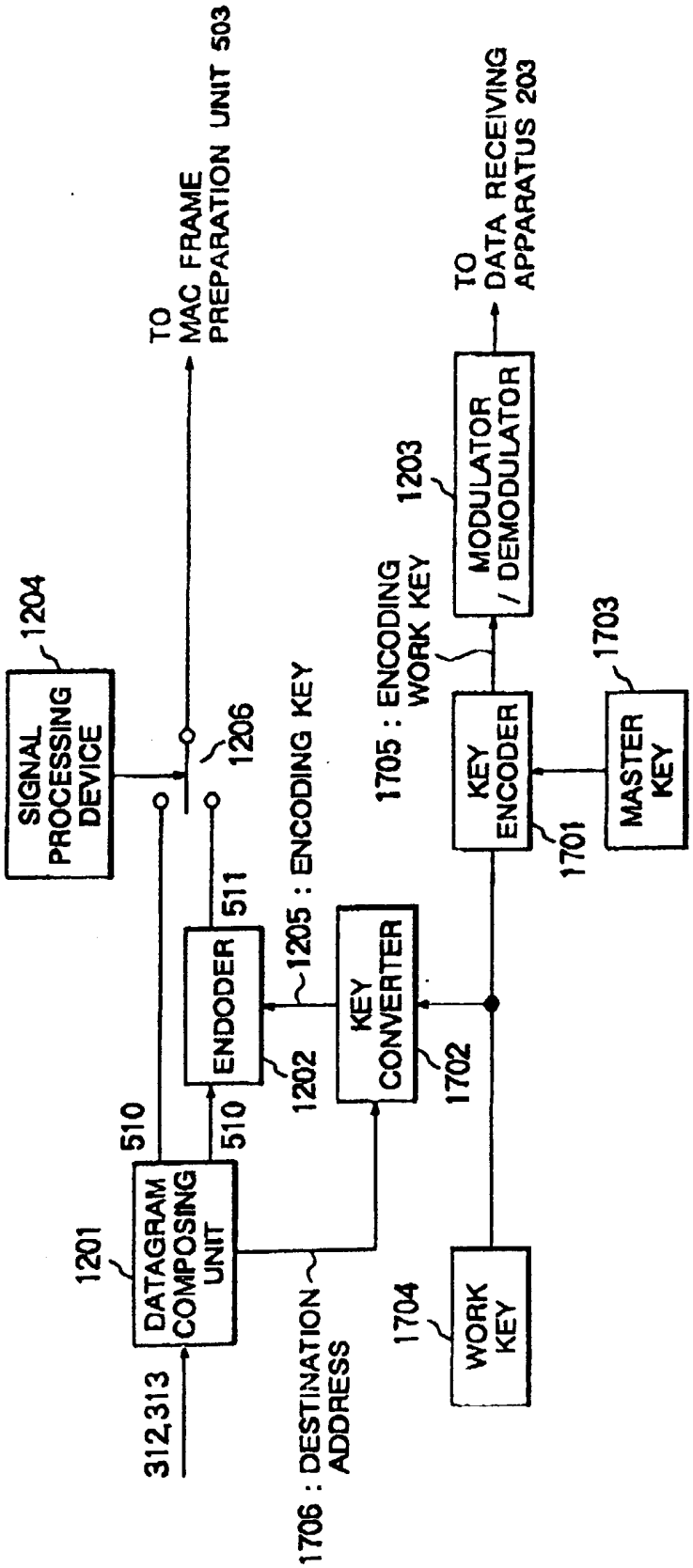

TO MAC FRAME PREPARATION UNIT 503
TO DATA RECEIVING APPARATUS 203
SIGNAL PROCESSING DEVICE
1204
1206
MODULATOR / DEMODULATOR
1203
1705 : ENCODING WORK KEY
KEY ENCODER
1701
MASTER KEY
1703
511
ENDODER
1202
1205 : ENCODING KEY
KEY CONVERTER
1702
510
510
DATAGRAM COMPOSING UNIT
1201
312,313
1706 : DESTINATION ADDRESS
WORK KEY
1704

FIG. 18

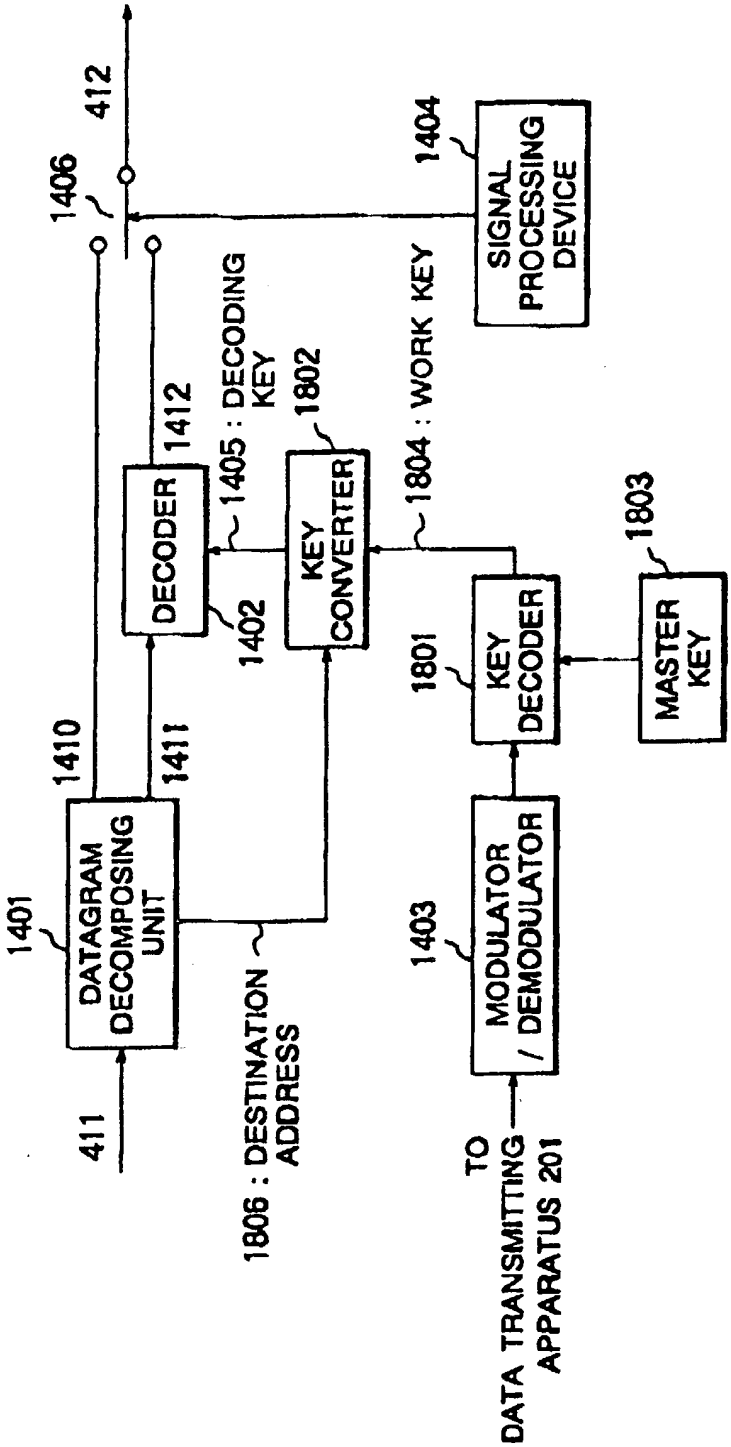

411
DATAGRAM DECOMPOSING UNIT
1401
1410
1411
DECODER
1412
1402
KEY CONVERTER
1802
1405 : DECODING KEY
1806 : DESTINATION ADDRESS
1406
412
1404
SIGNAL PROCESSING DEVICE
1804 : WORK KEY
1801
KEY DECODER
1803
MASTER KEY
1403
MODULATOR / DEMODULATOR
TO DATA TRANSMITTING APPARATUS 201

FIG. 19

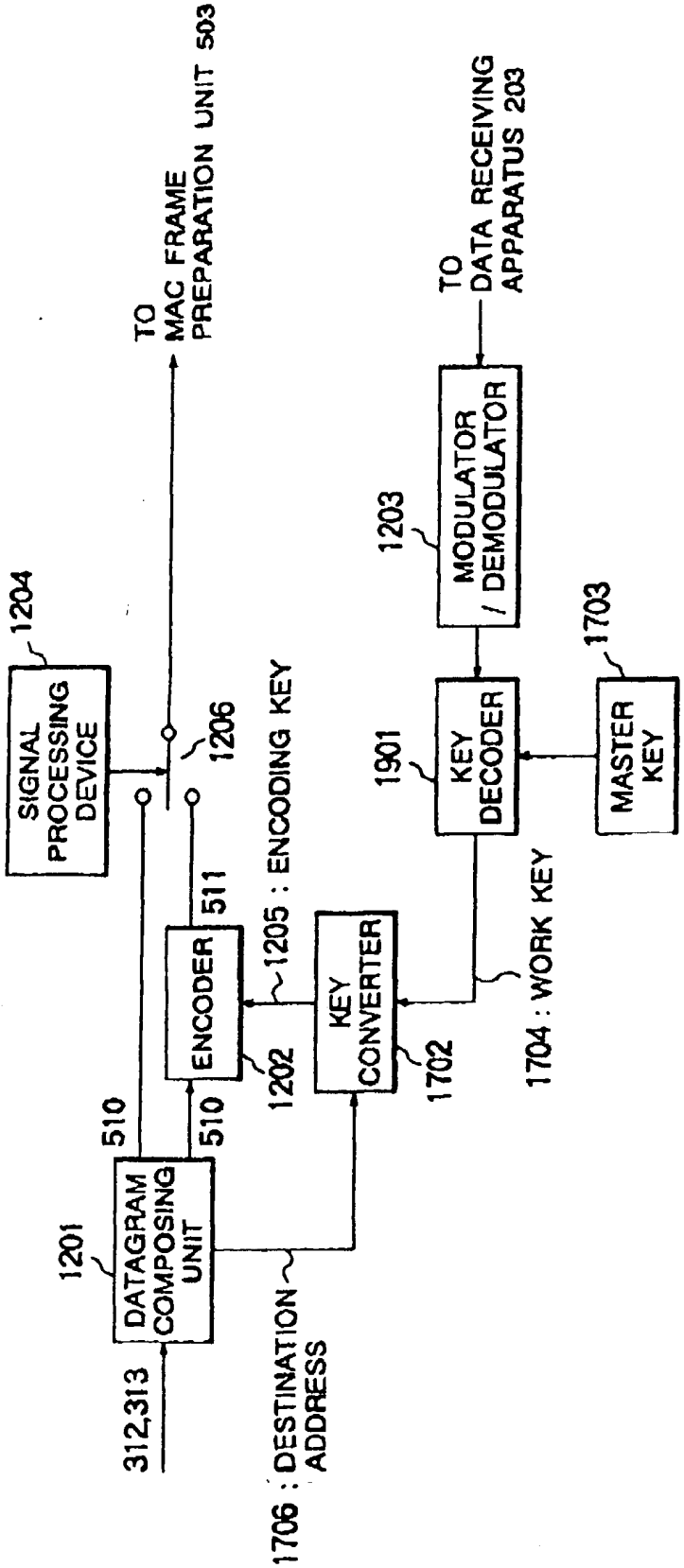

SIGNAL PROCESSING DEVICE
1204
TO MAC FRAME PREPARATION UNIT 503
1206
511
ENCODER
1205 : ENCODING KEY
1202
KEY CONVERTER
1702
1203
MODULATOR / DEMODULATOR
TO DATA RECEIVING APPARATUS 203
1901
KEY DECODER
1703
MASTER KEY
1704 : WORK KEY
510
510
1201
DATAGRAM COMPOSING UNIT
312,313
1706 : DESTINATION ADDRESS

FIG. 20

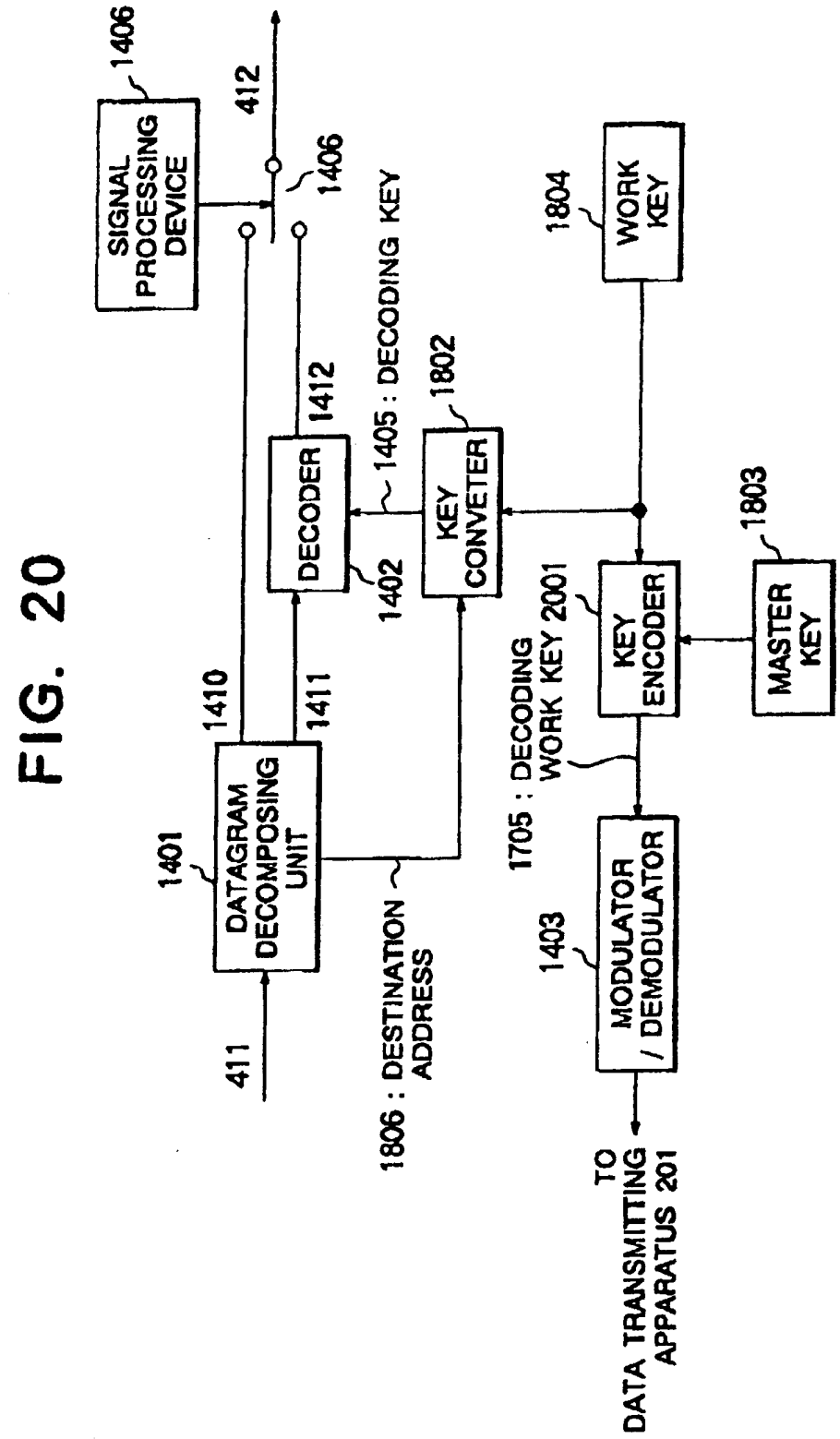

SIGNAL PROCESSING DEVICE
1406
412
1406
DECODER
1412
1405 : DECODING KEY
KEY CONVETER
1802
1804
WORK KEY
1410
1411
1402
1401
DATAGRAM DECOMPOSING UNIT
411
1806 : DESTINATION ADDRESS
1705 : DECODING WORK KEY 2001
KEY ENCODER
1803
MASTER KEY
1403
MODULATOR / DEMODULATOR
TO DATA TRANSMITTING APPARATUS 201

FIG. 21

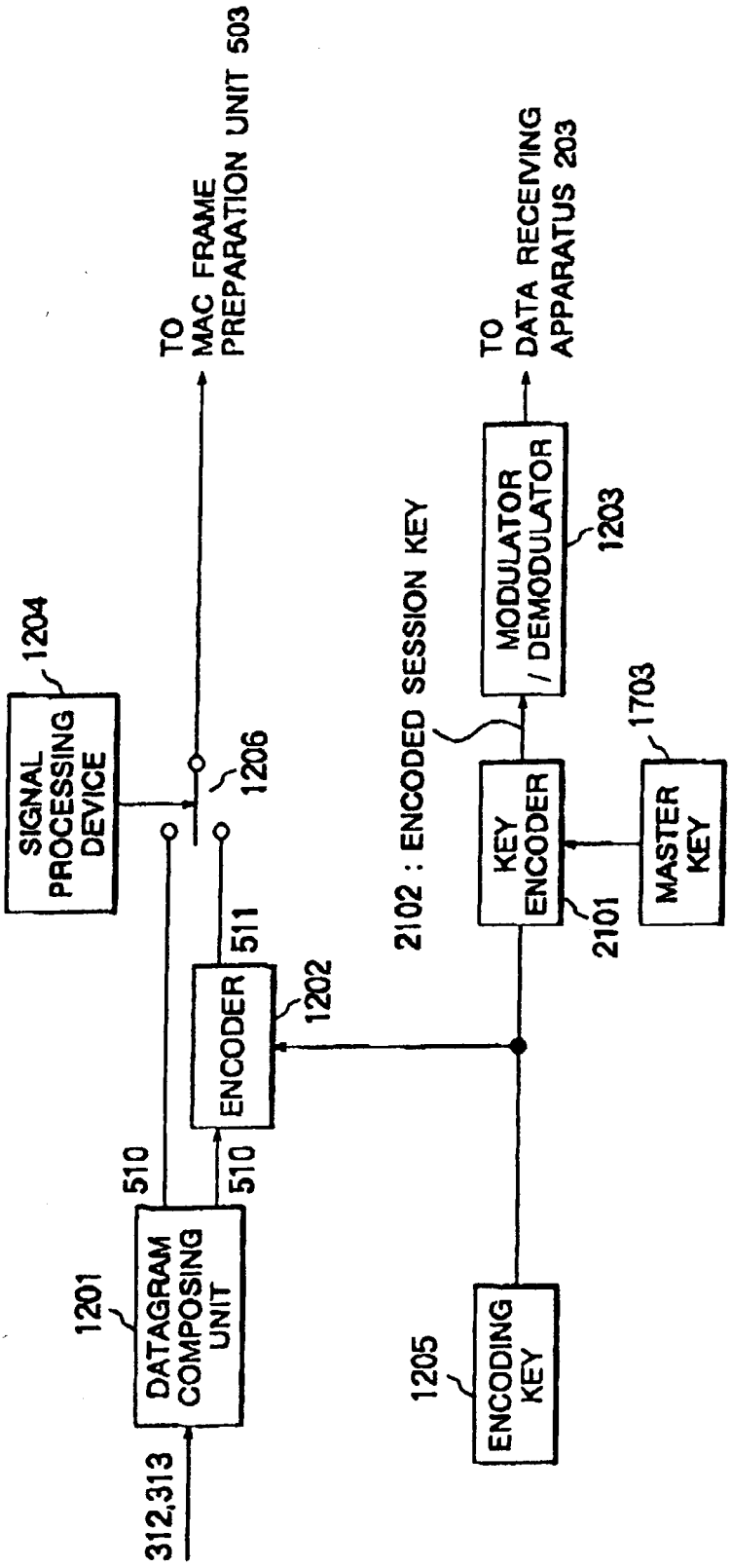

312,313
1201
DATAGRAM COMPOSING UNIT
510
510
511
ENCODER
1202
1204
SIGNAL PROCESSING DEVICE
1206
TO MAC FRAME PREPARATION UNIT 503
2102 : ENCODED SESSION KEY
1205
ENCODING KEY
KEY ENCODER
2101
MASTER KEY
1703
MODULATOR / DEMODULATOR
1203
TO DATA RECEIVING APPARATUS 203

FIG. 22

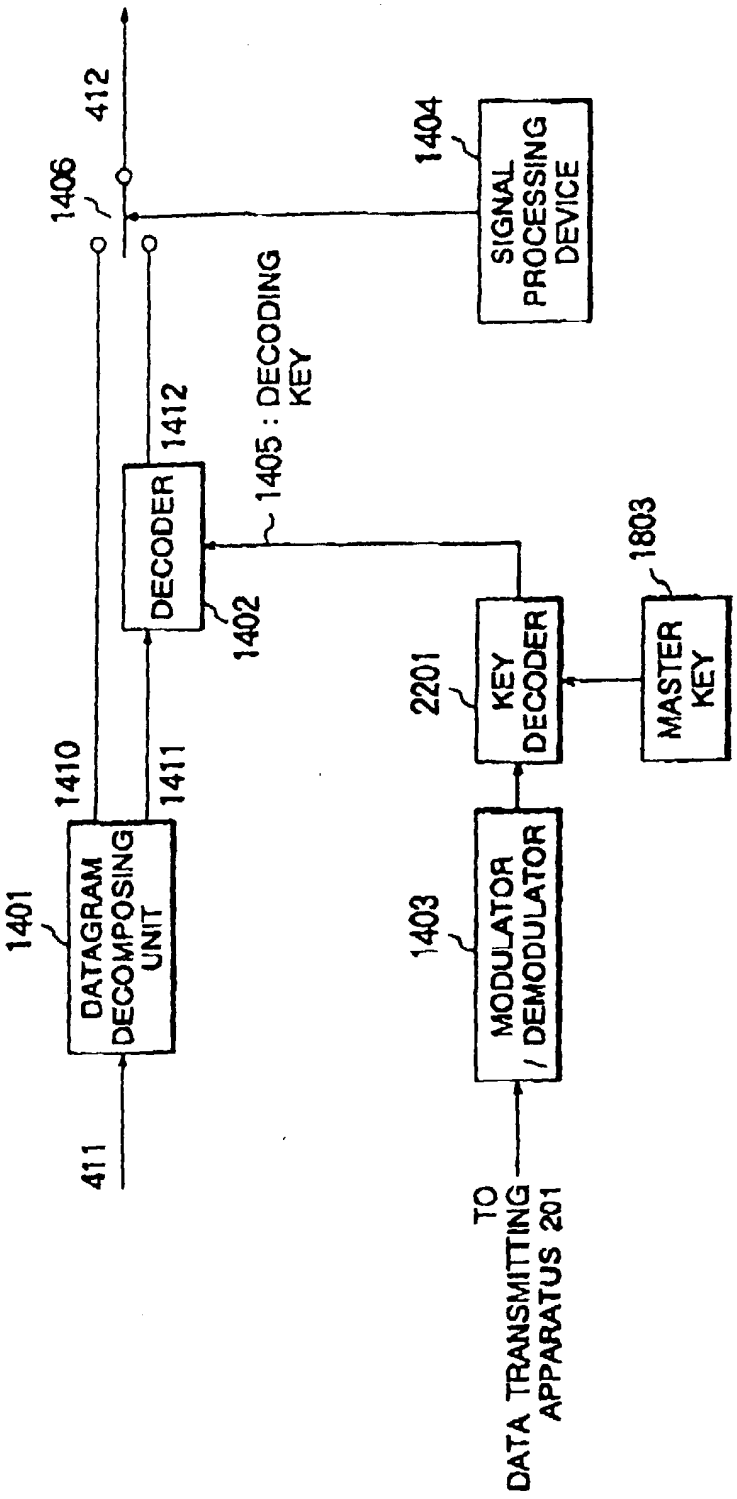

412
1406
1404
SIGNAL PROCESSING DEVICE
1405 : DECODING KEY
1412
DECODER
1402
1410
1411
1401
DATAGRAM DECOMPOSING UNIT
411
2201
KEY DECODER
1803
MASTER KEY
1403
MODULATOR / DEMODULATOR
TO DATA TRANSMITTING APPARATUS 201

FIG. 23

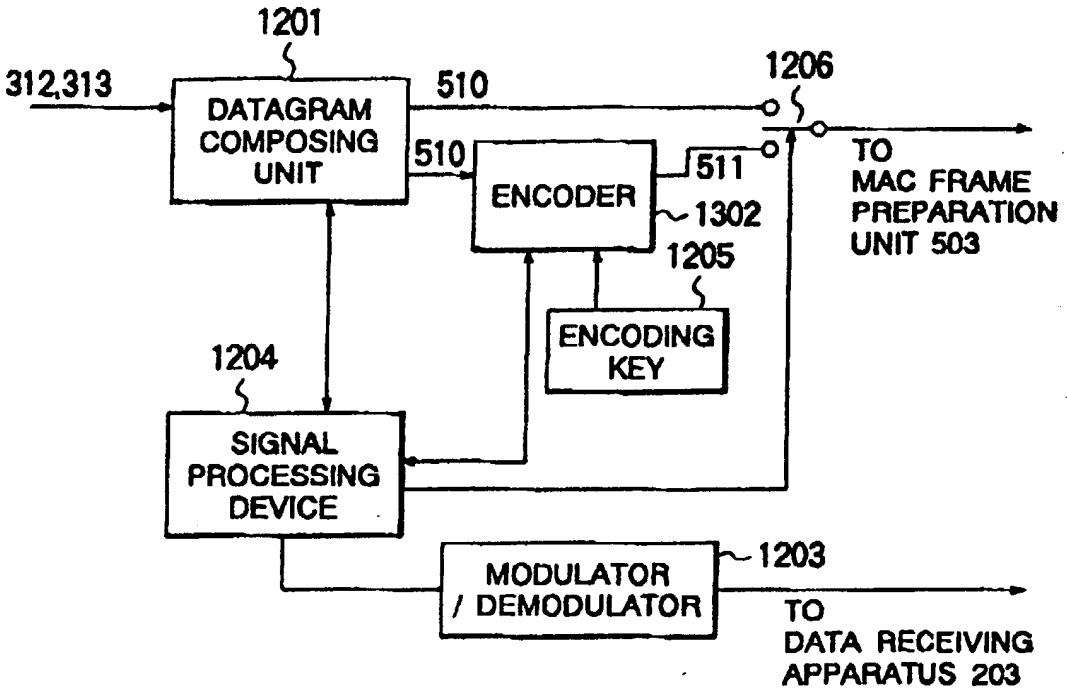
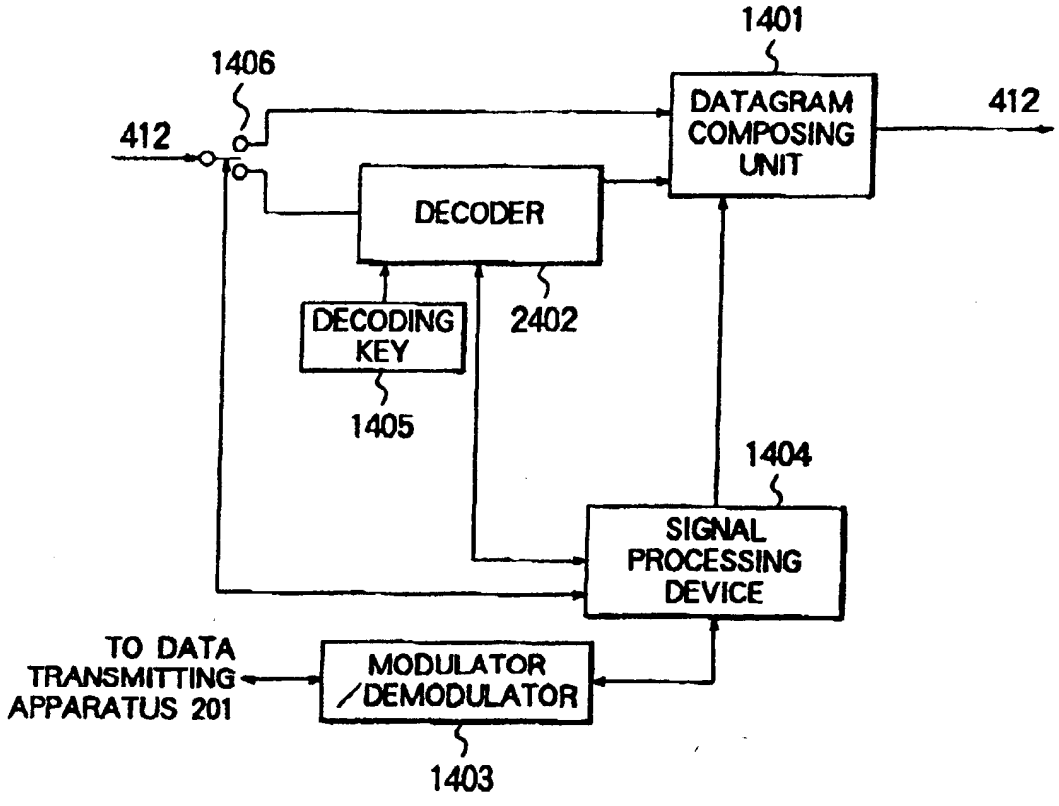

1201
312,313
DATAGRAM COMPOSING UNIT
510
1206
510
ENCODER
511
1302
1205
TO MAC FRAME PREPARATION UNIT 503
ENCODING KEY
1204
SIGNAL PROCESSING DEVICE
MODULATOR / DEMODULATOR
1203
TO DATA RECEIVING APPARATUS 203

FIG. 24


1401
1406
412
DATAGRAM COMPOSING UNIT
412
DECODER
DECODING KEY
2402
1405
1404
SIGNAL PROCESSING DEVICE
TO DATA TRANSMITTING APPARATUS 201
MODULATOR /DEMODULATOR
1403

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP97/00850

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl^6 G09C1/00, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl^6 G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1940 - 1997 Jitsuyo Shinan Toroku Koho 1996 - 1997
Kokai Jitsuyo Shinan Koho 1971 - 1997
Toroku Jitsuyo Shinan Koho 1994 - 1997

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 01-231490, A (Victor Co. of Japan, Ltd.), September 14, 1989 (14. 09. 89), Claim; page 1, right column, lines 4 to 7 (Family: none)	1 - 80
Y	JP, 07-283809, A (Mitsubishi Corp.), October 27, 1995 (27. 10. 95), Page 3, right column, lines 6 to 30; Fig. 1 (Family: none)	1 - 80
Y	JP, 60-208137, A (Toshiba Corp.), October 19, 1985 (19. 10. 85), Page 2, lines 14 to 18; Fig. 5 (Family: none)	17-19, 36-38, 55-57, 74-76
Y	JP, 4-92886, U (NEC Home Electronics Ltd.), August 12, 1992 (12. 08. 92), Claim; Fig. 2 (Family: none)	15-16, 34-35, 53-54, 72-73
Y	JP, 5-292047, A (NEC Corp.), November 5, 1993 (05. 11. 93), Claim 1 (Family: none)	2-4, 20-23, 39-42, 58-61

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
June 3, 1997 (03. 06. 97)	June 17, 1997 (17. 06. 97)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP97/00850

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 4-274636, A (NEC Chugoku Software K.K.), September 30, 1992 (30. 09. 92), Figs. 2, 3 (Family: none)	10, 13, 15, 16, 29, 32, 34, 35, 48, 51, 53, 54, 67, 70, 72, 73
Y	JP, 6-152592, A (Hitachi, Ltd.), May 31, 1994 (31. 05. 94), Fig. 1; claim 1 (Family: none)	5, 6, 8, 24, 25, 27, 43, 44, 46, 62, 63, 65
Y	JP, 6-311157, A (Fujitsu Ltd.), November 4, 1994 (04. 11. 94), Page 3, right column, lines 10 to 18 (Family: none)	13, 14, 32, 33, 51, 52, 70, 71
Y	JP, 8-32574, A (Oki Electric Industry Co., Ltd.), February 2, 1996 (02. 02. 96), Claim 2 (Family: none)	1 - 80
Y	JP, 7-170280, A (Ricoh Co., Ltd.), July 4, 1995 (04. 07. 95), Page 4, left column, line 38 to right column, line 4; Figs. 1, 6; Table 1 (Family: none)	15, 16, 34, 35, 53, 54
Y	JP, 4-92887, U (NEC Home Electronics Ltd.), August 12, 1992 (12. 08. 92), Fig. 2 (Family: none)	15, 16, 34, 35, 53, 54
Y	JP, 6-37750, A (Hitachi, Ltd.), February 10, 1994 (10. 02. 94), Page 5, left column, lines 9 to 19 (Family: none)	5, 6, 24, 25, 43, 44, 62, 63
Y	JP, 6-303231, A (Pumpkin House Inc.), October 28, 1994 (28. 10. 94), Page 2, lines 27 to 46 (Family: none)	8, 9, 27, 28, 46, 47, 65, 66, 18, 19, 37, 38, 56, 57, 75, 76 18, 19, 37, 38, 56, 57, 75, 76
Y	JP, 7-107082, A (Nippon Telegraph & Telephone Corp.), April 21, 1995 (21. 04. 95), Figs. 1, 6; page 4, left column, line 38 to right column, line 4 (Family: none)	7, 9, 11, 14

Form PCT/ISA/210 (continuation of second sheet) (July 1992)